JP5224604A DEVICE FOR MANAGING PUBLIC KEY CIPHER SYSTEM

Bibliography

DWPI Title

Cryptographic system using public key private key pairs generates two key pairs using one known and one unknown seed value with corresponding control vectors to control use of key pairs.

Original Title

DEVICE FOR MANAGING PUBLIC KEY CIPHER SYSTEM

Assignee/Applicant

Standardized: IBM
Original: INTERNATL BUSINESS MACH CORP <IBM>

Inventor

MATYAS STEPHEN M ; JOHNSON DONALD B ; LE AN V ; WILLIAM C MARTIN ; ROSTISLAW PRYMAK ; JOHN D WILKINS

Publication Date (Kind Code)

1993-09-03 (A)

Application Number / Date

JP1992231284A / 1992-08-06

Priority Number / Date / Country

US1991766533A / 1991-09-27 / US
JP1992231284A / 1992-08-06 / JP

Abstract

PURPOSE: To make a user port public and private keys from a certain cipher system to another cipher system and improve security protection, by generating a pair of the public key and the private key from a path phrase first.

CONSTITUTION: This device is provided with a cipher facility 30, a cipher key data set 32, a ciphering mechanism access program 24 and an application program 36. Then, the first pair of the public key and the private key is generated by using a first seed value known to the user and a first control vector for defining the first private use of the first pair of the public key and the private key is generated. Then, the second pair of the public key and the private key is generated by using a second seed value known to the user and a second control vector for defining the second private use of the second pair of the public key and the private key is generated. Then, the private use of the first pair of the public key and the private key is controlled by using the first control vector and the private use of the second pair of the public key and the private key is controlled by using the second control vector.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－224604

(43)公開日　平成5年(1993)9月3日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ　1/00		9194－5L			
Ｈ０４Ｌ　9/06					
9/14					
		7117－5K	Ｈ０４Ｌ	9/ 02	Ｚ

審査請求　有　　請求項の数15(全 31 頁)

(21)出願番号　特願平4－231284

(22)出願日　平成4年(1992)8月6日

(31)優先権主張番号　７６６５３３

(32)優先日　1991年9月27日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　スティーブン、エム、マティアス
アメリカ合衆国バージニア州、マナサス、シーダー、リッジ、ドライブ、10298

(74)復代理人　弁理士　佐藤　一雄　（外５名）

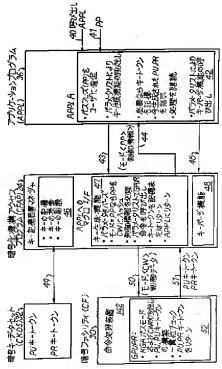
最終頁に続く

(54)【発明の名称】　パスフレーズを用いて公用および私用キーペアを生成する方法およびその装置

(57)【要約】　（修正有）

【目的】　パスフレーズを用いて公用、私用のキーを生成し、機密保護を高める。

【構成】　ユーザに知られた第１のシード値を用いて第１の公用キー、私用キーペアを生成し、第１の公用キー、私用キーペアの第１の使用を定義する第１の制御ベクトルを生成する。次に、ユーザに知られない第２のシード値を用いて第２の公用キー、私用キーペアを生成するステップを継続し、第２の公用キー、私用キーペアの第２使用を定義する第２の制御ベクトルを生成する。次に、第１の制御ベクトルを用いて第２の公用キー、私用キーペアの使用を制御し、また第２の制御ベクトルによって第２公用キー、私用キーペアの使用を制御する。



【特許請求の範囲】
【請求項１】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、
ユーザに知られている第１のシード値を用いて第１の公用キー、私用キーペアを生成し、また前記第１の公用キー、私用キーペアの第１の使用を定義する第１の制御ベクトルを生成するステップと、
ユーザに知られている第２のシード値を用いて第２の公用キー、私用キーペアを生成し、また前記第２の公用キー、私用キーペアの第２の使用を定義する第２の制御ベクトルを生成するステップと、
前記第１の制御ベクトルを用いて前記第１の公用キー、私用キーペアの使用を制御するステップと、
前記第２の制御ベクトルを用いて前記第２の公用キー、私用キーペアの使用を制御するステップとを含むことを特徴とする方法。
【請求項２】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、
パスフレーズから導出される第１のシード値を用いて第１の乱数を生成するステップと、
ユーザには知られない第２のシード値を用いて第２の乱数を生成するステップと、
前記第１の乱数を用いて第１の公用キー、私用キーペアを生成し、また前記第１の公用キーおよび前記第１の私用キーの第１の使用を定義するために、それぞれ第１の公用キー制御ベクトルおよび第１の私用キー制御ベクトルを生成するステップと、
前記第２の乱数を用いて第２の公用キー、私用キーペアを生成し、また前記第２の公用キーおよび前記第２の私用キーの第２の使用を定義するために、それぞれ第２の公用キー制御ベクトルおよび第２の私用キー制御ベクトルを生成するステップと、
前記第１の公用キー制御ベクトルおよび前記第１の私用キー制御ベクトルを用いて、それぞれ前記第１の公用キーおよび前記第１の私用キーの使用を制御するステップと、
前記第２の公用キー制御ベクトルおよび前記第２の私用キー制御ベクトルを用いて、それぞれ前記第２の公用キーおよび前記第２の私用キーの使用を制御するステップとを含むことを特徴とする方法。
【請求項３】データ処理システムにおいて、キー発生器を有する暗号システムを管理する方法であって、
パスフレーズから導出される第１のシード値を用いて第１の乱数を生成するステップと、
ユーザに知られない第２のシード値を用いて第２の乱数を生成するステップと、
前記第１の乱数を用いて第１キーを生成し、また前記第１のキーの使用を制御するための第１の制御ベクトルを生成するステップと、
前記第２の乱数を用いて第２のキーを生成し、また前記第２のキーの第２の私用を制御するための第２の制御ベクトルを生成するステップと、
前記第１の制御ベクトルにより前記第１のキーの使用を制御するステップと、
前記第２の制御ベクトルにより前記第２のキーの使用を制御するステップと、
前記第１のキーの前記第１の使用が、前記第２のキーの前記第２の使用と異なるステップとを含むことを特徴とする方法。
【請求項４】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出される第１のシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成し、前記第１の制御ベクトルは前記公用キーの使用を制御するもので、前記第２の制御ベクトルは前記私用キーの使用を制御するものであり、前記公用キーに対して前記第１の制御ベクトルを生成し、また前記私用キーに対して前記第２の制御ベクトルを生成するためのステップを含むことを特徴とする方法。
【請求項５】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出されるシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成するステップとを含むことを特徴とする方法。
【請求項６】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、
ユーザに知れている第１のシードを用いて第１の公用キー、私用キーペアを生成し、また前記第１の公用キー、私用キーペアの第１の使用を定義する第１の制御ベクトルを生成するステップと、
ユーザに知れない第２のシード値を用いて第２の公用キー、私用キーペアを生成し、また前記第２の公用キー、私用キーペアの第２の使用を定義する第２の制御ベクトルを生成するステップと、
前記第１の制御ベクトルを用いて前記第１の公用キー、私用キーペアの使用を制御するステップと、
前記第２の制御ベクトルにより前記第２の公用キー、私用キーペアの使用を制御するステップとを含む方法を実行することを特徴とする方法。
【請求項７】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出される第１のシード値を用いて第

１の乱数を生成するステップと、
ユーザに知られない第２のシード値を用いて第２の乱数を生成するステップと、
前記第１の乱数を用いて第１の公用キー、私用キーペアを生成し、また前記第１の公用キーおよび前記第１の私用キーの第１の使用をそれぞれ定義するための第１の公用制御キーベクトルおよび第２の私用キー制御ベクトルを生成するステップと、
前記第２の乱数を用いて第２の公用キー、私用キーペアを生成し、また前記第２の公用キーおよび前記第２の私用キーの第２の使用をそれぞれ定義するために、第２の公用キー制御ベクトルおよび第２の私用キー制御ベクトルを生成するステップと、
前記第１の公用キー制御ベクトルおよび前記第１の私用キー制御ベクトルを使用して、それぞれ前記第１の公用キーおよび前記第１の私用キーの前記第１の使用を制御するステップと、
前記第２の公用キー制御ベクトルおよび前記第２の私用キー制御ベクトルを使用して、それぞれ前記第２の公用キーおよび前記第２の私用キーの使用を制御するステップとを含むことを特徴とする方法。
【請求項８】データ処理システムにおいて、キー発生器を有する暗号システムを管理するための方法であって、
パスフレーズから導出される第１のシード値を用いて第１の乱数を生成するステップと、
ユーザに知られない第２のシード値を用いて第２の乱数を生成するステップと、
前記第１の乱数を用いて第１のキーを生成し、また前記第１のキーの使用を制御するための第１の制御ベクトルを生成するステップと、
前記第２の乱数を用いて第２のキーを生成し、また前記第２のキーの第２の使用を制御するための第２の制御ベクトルを生成するステップと、
前記第１の制御ベクトルにより前記第１のキーの使用を制御するステップと、
前記第２の制御ベクトルにより前記第２のキーの使用を制御するステップと、
前記第１のキーの第１の使用が前記第２のキーの前記第２の使用とは異なっているステップとを含むことを特徴とする方法。
【請求項９】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出される第１のシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第１の制御ベクトルおよび前記私用キーに対する第２の制御ベクトルを生成し、前記第１の制御ベクトルが前記公用キーの使用を制御し、前記第２の制御ベクトルが前記私用キーの使用を制御するステップとを含むことを特徴とする方法。
【請求項１０】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出されるシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成するステップとを含むことを特徴とする方法。
【請求項１１】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
ユーザに知られる第１シード値を用いて第１公用キー、私用キーペアを生成し、また前記第１公用キー、私用キーペアの第１使用を定義する第１制御ベクトルを生成する第１生成手段と、
ユーザに知られない第２シード値を用いて第２公用キー、私用キーペアを生成し、また前記第２公用キー、私用キーペアの第２使用を定義する第２制御ベクトルを生成する第２生成手段と、
前記第１制御ベクトルを用いて前記第１公用キー、私用キーペアの使用を制御するための、前記第１生成手段に連結される制御手段と、
前記第２制御ベクトルにより前記第２公用キー、私用キーペアの使用を制御するための、前記第２生成手段に連結される前記制御手段とを含むことを特徴とする装置。
【請求項１２】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
パスフレーズから導出される第１シード値を用いて第１乱数を生成するための第１生成手段と、
ユーザに知られない第２シード値を用いて第２乱数を生成するための第２生成手段と、
前記第１乱数を用いて第１公用キー、私用キーペアを生成し、また前記第１公用キーおよび前記第１私用キーの第１使用をそれぞれ定義するための第１公用キー制御ベクトルおよび第１私用キー制御ベクトルを生成する前記第１生成手段と、
前記第２乱数を用いて第２公用キー、私用キーペアを生成し、また前記第２公用キーおよび前記第２私用キーの第２使用をそれぞれ定義するための第２公用キー制御ベクトルおよび第２私用キー制御ベクトルを生成する前記第２生成手段と、
前記第１公用キー制御ベクトルおよび前記第１私用キー制御ベクトルをそれぞれ用いて、前記第１公用キーおよび前記第１私用キーの使用を制御するための、前記第１生成手段に連結される制御手段と、
前記第２公用キー制御ベクトルおよび前記第２私用キー制御ベクトルをそれぞれ用いて、前記第２公用キーおよび前記第２私用キーの使用を制御するための、前記第２生成手段に連結される制御手段とを含むことを特徴とす

る装置。

【請求項１３】データ処理システムにおいて、キー発生器を有する暗号システムを管理するための装置であって、

パスフレーズから導出される第１シード値を用いて第１乱数を生成するための第１生成手段と、

ユーザに知られない第２シード値を用いて第２乱数を生成するための第２生成手段と、

前記第１乱数を用いて第１キーを生成し、また前記第１キーの使用を制御するための第１制御ベクトルを生成する前記第１生成手段と、

前記第２乱数を用いて第２キーを生成し、また前記第２キーの第２使用を制御するための第２制御ベクトルを生成する前記第２生成手段と、

前記第１制御ベクトルでもって前記第１キーの使用を制御するための前記第１生成手段に連結される制御手段と、

前記第２制御ベクトルでもって前記第２キーの使用を制御するための前記第２生成手段に連結される前記制御手段と、

前記第１キーの前記第１使用が前記第２キーの前記第２使用と異なることを含むことを特徴とする装置。

【請求項１４】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、

パスフレーズから導出される第１シード値を用いて乱数を生成する生成手段と、

前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第１制御ベクトルおよび前記私用キーに対する第２制御ベクトルを生成し、前記第１制御ベクトルが前記公用キーの使用を制御し、前記第２制御ベクトルが前記私用キーの使用を制御する前記生成手段とを含むことを特徴とする装置。

【請求項１５】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、

パスフレーズから導出されるシード値を用いて乱数を生成する生成手段と、

前記乱数を用いて公用キー、私用キーペアを生成する前記生成手段とを含むことを特徴とする装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、広くはデータ処理のシステムと方法、更に詳しくは機密保護を高めるためデータ処理システムに於て使用する暗号システムおよび方法に関する。

【０００２】

【従来の技術およびその課題】以下の特許および同時系属出願の特許明細書は本発明に関連し参考としてここに記載する。

【０００３】B. Brachtl 等の「生成ステーション設定制御値を経由する暗号キーの制御的使用」ＵＳＰ　４，８５０，０１７（１９８９年７月１８日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「制御ベクトルを用いるキーの機密保護管理」ＵＳＰ　４，９４１，１７６（１９９０年７月１０日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「制御ベクトルを用いるデータ暗号演算」ＵＳＰ　４，９１８，７２８（１９９０年４月１７日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「制御ベクトルを用いる個人識別番号処理」ＵＳＰ　４，９２４，５１４（１９９０年５月８日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「拡張制御キーを用いるキーの機密保護管理」ＵＳＰ　４，９２４，５１５（１９９０年５月８日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「制御ベクトル変換を用いる機密保護キー管理」ＵＳＰ　４，９９３，０６９（１９９１年２月１２日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「プログラム可能な制御ベクトル検査を用いる機密保護キー管理」ＵＳＰ　５，００７，０８９（１９９１年４月９日、譲受人　ＩＢＭ Corporation ）

B. Brachtl 等の「公用一方向暗号化機能に基く修正検出コードを用いるデータ認証」ＵＳＰ　４，９０８，８６１（１９９０年３月３日、譲受人　ＩＢＭ Corporation ）

D. Abraham 等「外部プログラム能力を有するスマートカードおよび同じくつくる方法」出願番号００４，５０１（１９８７年１月１９日ファイル、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「ＲＳＡ暗号変数記憶装置を圧縮する手法」ＵＳＰ　４，７３６，４２３（１９８８年４月５日、譲受人　ＩＢＭ Corporation ）

S. Schulzの「乱数発生器回路」ＵＳＰ　４，９０５，１７６（１９９０年２月２７日、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「多重パス検査により制御ベクトルを用いるキーの機密保護管理」出願番号０７／５９６，６３７（１９９０年１０月１２日ファイル、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「制御ベクトル実施の代替モードを用いる安全な暗号演算」出願番号０７／５７４，０１２（１９９０年８月２２日ファイル、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「キーに対するインポート完全性レベルに基き、公用キーの使用を制御する方法および装置」出願番号０７／６０２，９８９（１９９０年１０月２４日ファイル、譲受人　ＩＢＭ Corporation ）

S. M. Matyas 等の「制御ベクトルに基づくハイブリッド

公用キーアルゴリズム／データ暗号化アルゴリズムキー分散法」出願番号０７／７４８，４０７（１９９１年８月２２日ファイル、譲受人　ＩＢＭ　Corporation）S.M. Matyas 等の「制御ベクトルに基づく公用キー暗号システムキー管理」（本特許出願と同日出願、譲受人　ＩＢＭ　Corporation）引用したS.M. Matyas 等による特許に述べられている暗号体系は暗号キーとキーの創案者が意図するキーの使用に対し認証を与える制御ベクトルとの連繋に基づいている。S.M. Matyas 等による引用特許に述べられている暗号体系はデータ暗号化アルゴリズム（ＤＥＡ）（米国標準規格×３．９２－１９８１、データ暗号化アルゴリズム、米国標準規格協会、New York（１９８１年１２月３１日）参照）に基づいているのに対し、本発明はＤＥＡ等の機密キーと公用キーアルゴリズムの両方に基づいている。本発明に従って、各種キー管理機能、データ暗号機能、その他データ処理機能が制御ベクトルを用いて可能である。システム管理者は本発明に従う適当な制御ベクトルを選択することにより、その機密保護方針の実施に当って柔軟性を発揮することが出来る。暗号体系中の暗号ファシリティ（ＣＦ）は前に引用したS.M. Matyas 等の特許中に述べられている。ＣＦは暗号命令の集合に対する命令処理装置であって、暗号化方法およびキー生成方法を実行する。暗号ファシリティにおける記憶装置が内部暗号変数の集合を記憶する。各暗号命令は入力パラメータの集合を出力パラメータの集合に変換するのに必要な一連の処理ステップに関し述べられている。暗号ファシリティアプリケーションプログラム（ＣＦＡＰ）もまた参照された特許および出願明細書中に述べられており、これは対応する入力および出力パラメータと共に命令略号およびアドレスからなる各暗号命令に対する呼び出し方法を（呼び出し順序として）定義する。

【０００４】公用キー暗号化アルゴリズムはW.Diffie、M.E.Hellman 共著の「プライバシーと認証：暗号入門“Privacy and Authentication:An Introduction to Cryptography”」米国電気電子学会誌（ＩＥＥＥ）、６７巻３号、１９７９年３月、pp. ３９７～４２７に述べられている。公用キーシステムは、機密分散チャネルが充分な完全性レベルを有する限り、そのチャネルなしですますことを基にしている。公用キー暗号システムでは、２種のキーが使用され、その１は暗号化用であり他の１は解読用である。公用キーアルゴリズムは(1) インバースキーＰＵ（暗号化用）およびＰＲ（解読用）の無作為ペアを生成するのが容易であり、(2) ＰＵ、ＰＲによる演算が容易であるが、(3) ＰＵからＰＲを計算することは計算上は実行不可能であるように設計されている。ユーザは解読変換ＰＲを機密に保ち、暗号化変換ＰＵは、それを公用辞書におくことで公用する。誰でもメッセージを暗号化してそれをユーザに送信できるが、他の誰も彼に向けられたメッセージを解読は出来ない。ＰＵでもって暗号化し、ＰＲでもって解読することが可能であり、屡々望まれる。この理由で、ＰＵは一般に公用キーと呼び、ＰＲを一般に私用キーと呼ぶ。公用キー暗号システムの系特徴はメッセージの送信者を独特に識別するディジタル署名を提供することである。もしユーザＡが署名ずみのメッセージＭをユーザＢに送信しようと思うと、彼は彼の私用キーＰＲでその上に操作し、署名ずみメッセージＳを作成する。ＰＲは機密が望ましい時はＡの解読キーとして用いられたが、ここでは彼の「暗号化」キーとして用いる。ユーザＢがメッセージＳを受信すると、彼はＡの公用ＰＵでもって暗号文Ｓに操作してメッセージＭを回復できる。Ａのメッセージを連続的に解読することにより、受信者Ｂはそれが送信者Ａから来たという確証を得る。公用キー暗号の例は次の米国特許、Hellman 等のＵＳＰ　４，２１８，５８２「公用キー暗号装置および方法」、Hellman 等のＵＳＰ　４，２００，７７０「暗号装置および方法」、Rivest等のＵＳＰ　４，４０５，８２９「暗号通信システムおよび方法」に与えられている。

【０００５】たいていの暗号システムにおいては、一旦暗号キーが生成されると、暗号キーデータセットの中に暗号化した形で記憶することが出来るし、または生成装置から受信装置に暗号化した形で伝送し、そこで受信装置での記憶および使用に適当な形に再暗号化することも出来る。適当な媒体（例えばディスケット、磁気テープ、メモリカード、スマートカード）にキーを書き込み、その媒体を移送することにより、またはキーを電子的に伝送することによりある装置から他の装置にキーはポートされる。しかし、移送または伝送されているキーが対称キー暗号化アルゴリズム（例：データ暗号化アルゴリズム）と共に用いられる機密キーのような機密キーであるか、または非対称キー暗号アルゴリズムと共に用いる公用および私用キーペアの私用キーである時には、キーが敵により傍受されるかも知れない危険が常に存在する。機密または私用キーを安全に移送または伝送する一つの方法は、送信装置と受信装置間で共有するキーで、それらを暗号化することである。しかし、送信、受信装置がかかる機密保護暗号化チャネルを容易にするであろうキーを共有していない場合、または送信、受信装置がかかる機密保護チャネルを容易化するためにかかるキーイング関係を設定するのが不便あるいは不可能な場合がある。従って機密キーをある装置から他の装置にポートする唯一の便利な方法はクリアキーをポートすることしかないことがたびたびある。

【０００６】

【課題を解決するための手段】

本発明の目的

本発明の目的は、ユーザが公用および私用キーをある暗号システムから別の暗号システムにポートする改良された方法を提供することにある。

【０００７】本発明の別の目的はディスケット、磁気テープ、メモリカード、またはスマートカード等の分離した記憶媒体を必要とすることなく、ユーザがある暗号システムから別の暗号システムに公用および私用キーをポートすることが出来るようにすることにある。

【０００８】本発明の更に別の目的はユーザの公用および私用キーを生成し、ユーザが暗号装置を実際に使用中の期間に使用することができ、また、ユーザが暗号装置を不使用中はそのキーを暗号装置からパージすることができるようにすることにある。

【０００９】本発明の更に別の目的はユーザが暗号サービスを必要とする期間中は暗号能力を有するポータブルコンピュータ内で、ユーザの公用および私用キーを初期化し、また暗号システムが必要とされない時はそのキーをポータブルコンピュータからパージさせることにある。

【００１０】本発明の更に別の目的はパスフレーズ等のユーザが記憶している事柄だけから、ユーザの公用および私用キーペアを暗号装置ネットワーク内のいかなる暗号装置においても生成または再生成できる方法を提供することにある。

【００１１】本発明の更に別の目的はパスフレーズ組合わせ数が２の１２８ べき乗よりも大きく、なおそのパスフレーズがユーザが容易にそれを記憶できるような充分な冗長性を有することを保証するパスフレーズの構成法を提供することにある。

【００１２】本発明の更に別の目的はキー生成アルゴリズムがRivest-Shamir-Adelman （ＲＳＡ）公用キー暗号アルゴリズムに基づいているところで、入力パスフレーズから公用キーペアおよび私用キーペアを生成および再生成するための方法を提供することにある。

【００１３】本発明の更に別の目的はキー生成アルゴリズムがいかなる公用キー暗号アルゴリズムに基づいているところでも、入力パスフレーズから公用キーおよび私用キーペアを生成および再生成するための方法を提供することにある。

【００１４】本発明の更に別の目的はキー生成アルゴリズムにパスフレーズに基づかない第１のタイプ、およびパスフレーズに基づく第２のタイプの公用キーおよび私用キーペアを作成させるキー管理システムを提供することにある。

【００１５】本発明の別の目的はパスフレーズに基づかない第１のタイプの公用および私用キーペアには、第１のキー使用法が許されたキー使用法の第１の集合に基づくようにせしめ、またパスフレーズに基づく第２タイプの公用キーおよび私用キーペアには、第１のキー使用法が許されたキー使用法の第２の集合に基づくようにせしめるキー管理システムを提供することにある。

【００１６】本発明の別の目的はパスフレーズから生成される公用キーおよび私用キーは、パスフレーズから生成されない公用キーおよび私用キーとは暗号的に分離することができ、従ってパスフレーズから生成される公用キーおよび私用キーにより両タイプの生成される公用キーおよび私用キーを利用する暗号システムの全体機密保護を弱めることの起り得ないようなキー管理システムを提供することにある。

本発明の概要

上記その他の目的、特徴および効果はこゝに開示する本発明により達成される。本発明は暗号装置のネットワークにおいて、ある装置から他の装置に機密または公用キーをポートする代替手段を提供する。本発明はまた暗号装置のユーザが実際には暗号装置を使用していない間はその機密キーをパージし、また実際に暗号装置を使用している間は機密キーを再生成するための手段を提供する。これはユーザによりキー生成アルゴリズムに提供されるパスフレーズから公用キーおよび私用キーペアを先づ生成することにより達成される。その後同じキーペアの再生成が必要になるたびに、ユーザは同じパスフレーズを入力し、それからキー生成アルゴリズムが同じ公用キーおよび私用キーペアを導出する。かゝる手続きは暗号能力を有するポータブルのプログラマブルコンピュータ（ＰＣ）を所有する単一ユーザにより用いられる。ユーザが移動中はそのキーはシステムからパージされる。ユーザが暗号システムを使用中は、そのキーは再生成される。パスフレーズも、例えば８０文字以上と長いことがある点を除けば、考え方はパスワードと類似である。パスフレーズはより多くの文字を含みうるので、パスワードより多くの変異性を包含することができるが、ユーザがパスフレーズを記憶するのは容易である。

【００１７】図１は装置を使用中は公用キーおよび私用キーを生成し、不使用中はそのキーをパージしている２人のユーザｉ，ｊにより共有されている暗号システムＡのブロック図を示したものである。こゝで図１を参照し、時刻ｔ１に第１のユーザ（ユーザｉ）は自己のパスフレーズを入力しキー生成機能を呼び出すことにより自身の公用キーおよび私用キーＰＵｉ，ＰＲｉが暗号システムＡに再生成されるようにする。時刻ｔ０から時刻ｔ１まで、ユーザｉは暗号キーを実際に使用する。時刻ｔ１にユーザｉはキーパージ機能を呼び出して、公用キーおよび私用キーＰＵｉ，ＰＲ１をパージする。時刻ｔ２に、第２のユーザ（ユーザｊ）が自己のパスワードを入力しキー生成機能を呼び出すことにより、彼の公用キーおよび私用キーＰＵｊ，ＰＲｊが暗号システムＡに再生成されるようにする。時刻ｔ２から時刻ｔ３まで、ユーザｊは実際に自己の暗号キーを使用する。時刻ｔ３に、ユーザｊはキーパージ機能を呼び出して自己の公用キーおよび私用キーＰＵｊ，ＰＲｊをパージする。こゝで述べるキーパージ機能は公用キーおよび私用キーの両方ともパージしている。現実には、私用キーのみをパージすることで充分であろう。

【００１８】図２は単一ユーザｉがある装置使用を望むときは自己の公用キーおよび私用キーペアを生成し、その装置使用を終了すると自己のキーをパージする単一ユーザｉにより共用される暗号システムＡおよびＢのブロック図による説明である。こゝで図２を参照し、時刻ｔ０に、ユーザｉは自己のパスフレーズを入力しキー生成機能を呼び出すことにより、自己の公用キーおよび私用キーＰＵｉ，ＰＲｉがＡ暗号システムＡに再生成されるようにする。時刻ｔ０から時刻ｔ１まで、ユーザｉは実際に暗号キーを使用する。時刻ｔ１に、ユーザｉはキーパージ機能を呼び出すことにより、彼の公用キーおよび私用キーＰＵｉ，ＰＲｉをパージする。時刻ｔ１から時刻ｔ２まで、ユーザは暗号システムＡから暗号システムＢに移動する。時刻ｔ２に、ユーザｉは自己のパスフレーズを入力し、キー生成機能を呼び出すことにより自己の公用キーおよび私用キーＰＵｉ，ＲＶｉが暗号システムＢに再生成されるようにする。時刻ｔ２から時刻ｔ３までは、ユーザｉは暗号キーを実際に使用する。時刻ｔ３に、ユーザｉはキーパージ機能を呼び出すことにより公用キーおよび私用キーＰＵｉ，ＲＶｉをパージする。

【００１９】パスフレーズは自然言語例えば英語からとったワードまたはフレーズからなる。「時は風の如く、果実はバナナの如く飛ぶ」、「心配するな、悪いことなど起らない」、「父は弟に犬を買ってやった、弟はまだ子供だから」といったのがパスフレーズの例（必ずしも良い例ではないが）である。

【００２０】パスフレーズは意味をもったワードの列であるから、たとえパスフレーズが（空白を含み）８０文字以上を含んでいたとしても、ユーザがそのパスフレーズで記憶し思い出すことが出来る。こういう訳で、パスフレーズ組合せの数は容易に２の１２８べき乗（すなわち倍長ＤＥＡキーの組合せ数以上）を越えることができる。ユーザにはパスフレーズを作るための命令の集合またはガイドラインも同時に提供する。これによりユーザが不注意により敵が容易に推測できるようなパスフレーズを使用することがないようにする。例えば「メアリーは小羊をもっていて…」といったパスフレーズは長くても、最初の２ワードを知られると、残りは分ってしまう。「ドナルドダック，ジャックペニィ，アルフレッド大王がゴルフボールを食べながらチェスをした」といったパスフレーズは敵が推測できないことは、これを読めば容易に理解できる。キー生成中、キーを生成する過程でキー生成アルゴリズムが用いる所要の乱数を生成するシード値として、パスフレーズが用いられる。パスフレーズから生成する乱数以外には、いかなる乱数をもキー生成アルゴリズムは使用しない。生成された公用キーおよび私用キーペア（ＰＵ，ＰＲ）はパスフレーズのみに依存するので同じキー生成アルゴリズムを実行する暗号装置ネットワークの中ならばどの暗号装置でも（ＰＵ，ＰＲ）を再生成できる。ネットワークが単一の販売会社から購入した暗号装置から成立している場合、またはキー生成の方法が標準化されており、違う販売会社から入手する数種の製品に実行されている場合がこういった場合である。

【００２１】

【実施例】暗号システムのユーザが与える文字列からキーを生成するという概念はＩＢＭ社情報保護システム（ＩＰＳ）で実行してきたものであって、ＶＭ／ＣＭＳユーザガイド，Ｏｒｄｅｒ　Ｎｏ．ＳＨ２０－２６２１，ＩＢＭ　Ｃｏｒｐｏｒａｔｉｏｎ（１９８２年８月）の情報保護システム暗号プログラムを参照されたい。この情報保護システムは、データファイルを暗号化したり解読したりするのに用いるキーを暗号システムのユーザが制御，管理するという概念に基いて設計されたファイル保護システムである。システム自身のキーは一切ない。データの暗号化または解読が必要となった時に、ユーザが暗号システムにキーを規定してやらなければならない。ユーザは１６進数字キーまたは８０文字までの文字列のいずれかを規定すればよい。文字列が入力された場合は、ＩＰＳは次の方法により入力文字列を５６ビットキーに「クランチ」（なすわちハッシュ）する。入力文字列は８０文字の長さに空白つき右側に埋込まれる。次に入力文字列は８文字のブロックに分割される。その結果の埋込データはその値がＸ「０１０１０１０１０１０１０１」である一定キーおよびその値がＸ「００００００００００００００００」である初期チューニング値を用い、暗号化ブロック連鎖（ＣＢＣ）モードを用いてＤＥＡで暗号される。最終６４ビットブロックの暗号文の右端５６ビットが「クランチ」データキー（パリティビットなし）として取り上げられる。

【００２２】情報保護システムにおける文字列からデータキーを作成する方法は公用キーおよび私用キーペアの作成には拡張されない。公用キー生成アルゴリズムはより複雑なためである。ユーザが与えるパスフレーズから公用キーおよび私用キーペアを生成するためには、キー生成アルゴリズム自体を修正し、動的にシードされる擬似乱数発生器を使わなければならない。動的にシードされる擬似乱数発生器は発生器への入力として規定されるシード値から擬似乱数を生成するアルゴリズム処理手順である。かゝる擬似乱数発生器は暗号システムでの大抵の乱数を生成するのには通していない。というのは乱数発生器の呼出し者は、入力として規定さられるシード値を手許に持っていないか、または持たないことがよくあるからである。従って実際には、たいていの暗号システムでは動的にシードされる擬似乱数発生器を用いる便利な方法はない。代りに、これらの暗号システムでは初期にシードされる擬似乱数発生器または真の乱数を作成できる特殊ハードウェアを用いる。従って本発明の方法を実行するのが有利と考えられる所では、暗号システムは次の２つの乱数発生器を実行するのが必要であろう。

（１）は初期にシードされる擬似乱数発生器または真の乱数のハードウェア発生器であり、（２）は動的にシードされる擬似乱数発生器である。更に公用キーおよび私用キーが動的にシードされる擬似乱数発生器を利用して生成されることを許すキー生成アルゴリズムの設計を採用することが必要であろう。本発明のこれらの様子は以下に詳述する。

【００２３】前に引用したＵＳＰ４，７３６，４２３「ＲＳＡ暗号変数記憶装置」は５６ビットの機密値Ｘから５０ビットの非機密値Ｙを計算する方法を述べており、４００ビットモジュラスおよび４００ビット指数を有する公用キーおよび私用キーを再生成するのにその後いつでも使用できる。これ以上大きな指数およびモジュラス長に対しては、ｙの長さはＸが５６ビット一定に留っている間はほんの少し増加する。機密キー値Ｘはキー生成アルゴリズムへの入力として与えられ、公用キーおよび私用キーＰＵ，ＰＲの計算に加え、ｙの５０ビット値をも計算する。値ｙがＰＵ，ＰＲを生成するのに始めにかゝった時間に比べ、値ｙがＸと共に公用キーおよび私用ＲＳＡキーＰＵ，ＰＲを非常に迅速に再生成できるという点で、値ｙは特別である。この手法は一方ではＰＵ，ＰＲ（すなわち全指数とモジュラス）を記憶し、他方では必要になるたびにＰＵ，ＰＲを再生成するという両者間の妥協である。ＵＳＰ４，７３６，４２３の手法はキーを再生成する短い計算ステップを必要とする代りに記憶しなければならないビット数を減らしている。本発明では、公用キーおよび私用キーをユーザが記憶しているパスフレーズから全部生成する。ＵＳＰ４，７３６，４２３の方法が、入力パスフレーズをハッシュすることにより理論上は得られる５６ビットの独立変数Ｘを利用しているのと対照に、数値Ｙは５０ビットの従属変数である。すなわち公用キーおよび私用キーをポートするためには、ユーザは従属変数ｙをポートし、また暗号システムが公用および私用キーペアを再生成するように独立変数Ｘと共にそれを入力しなければならない。ＵＳＰ４，７３６，４２３は本発明の利点の一部は有しているが、本発明ではパスフレーズ以外の追加情報とは独立に、キーをある装置から別の装置に移送することが可能である。従って、本発明ではＵＰＳ４，７３６，４２３の方法では達成できないキーポートの形式が可能になる。

【００２４】こゝで開示する本発明の環境説明として、図３は通信ネットワーク１０を示すネットワークブロック図であり、これにデータ処理装置２０、データ処理装置２０′、データ処理装置２０″を含む多数のデータ処理装置が接続されている。また図３に示すように、各データ処理装置には暗号システムも含まれる。データ処理装置２０は暗号システム２２を含み、データ処理装置２０′は暗号システム２２′を含み、データ処理装置２０″は暗号システム２２″を含む。アプリケーションデータの暗号化、解読、認証や暗号キーの生成、導入等に対する暗号サービスへのアクセスを要する複数のアプリケーションの処理手順を、各データ処理装置がサポートする。暗号サービスは各暗号システムの安全な暗号化機構により与えられる。データ処理装置が暗号化したデータおよびキーを送受信する手段をネットワークが提供する。各種のプロトコル、すなわち書式と手順規則が通信用データ処理装置間の相互使用性を確保するためその間の暗号量の交換を支配する。

【００２５】図４はこゝで開示する発明の暗号システム２２を示す。暗号システム２２において、暗号化機構（ＣＦ）３０は物理的インタフェースからの入力３７を有している。暗号化機構アクセスプログラム（ＣＦＡＰ）３４がインタフェース３１により暗号化機構３０に結合される。暗号キーデータセット（ＣＫＤＳ）３２はインタフェース３３により暗号化機構アクセスプログラム３４に接続される。アプリケーションプログラム（ＡＰＰＬ）３６はアンタフェース３５により暗号化機構アクセスプログラム３４に接続される。

【００２６】典型的な暗号サービス要求はインタフェース３５にあるＣＦＡＰ３４への機能呼出しを通じＡＰＰＬ３６により開始する。サービス要求にはキーとデータパラメータならびにインタフェース３３のＣＫＤ３２から暗号化したキーにＣＦＡＰ３４がアクセスするのに用いるキー識別子を含んでいる。ＣＦＡＰ３４はインタフェース３１のＣＦ３０に複数の暗号アクセス命令を発行することによりサービス要求を処理する。ＣＦ３０にはＣＦ３０への暗号変数の直接入力のためのオプションの物理的インタフェース３７を有することもできる。ＣＦ３０によりＣＦＡＰ３４にリターンされる出力パラメータのセットを作成するために、ＣＦ３１に呼出される各暗号アクセス命令にはＣＦ３０により処理される入力パラメータのセットを有する。交替で、ＣＦＡＰ３４がＡＰＰＬ３６に出力パラメータをリターンすることも出来る。ＣＦＡＰ３４は以後の呼出し命令に出力パラメータおよび入力パラメータを使用することも可能である。もし出力パラメータが暗号化されたキーを含むならば、その時はＣＦＡＰ３４は、多くの場合これら暗号化されたキーをＣＫＤＳ３２に記憶することがある。

【００２７】図５はこゝで開示する本発明の暗号化機構３０を説明する。暗号化機構３０は機密保護範囲１４０内で保全される。暗号化機構３０には命令処理装置１４２を含み、これに実行コードとして具体化した暗号アルゴリズム１４４が結合している。暗号化機構環境記憶装置１４６は命令処理装置１４２に結合されている。図に示すように物理的インタフェースはライン３７を通してＣＦ環境記憶装置１４６に結合できる。命令処理装置１４２はインタフェース３１により暗号化機構アクセスプログラム（ＣＦＡＰ）３４に結合される。

【００２８】命令処理装置１４２はインタフェース３１

でＣＦＡＰアクセス命令により呼出された暗号マイクロ命令を実行する機能素子である。各アクセス命令に対し、インタフェース３１は実行用特別マイクロ命令の選択に用いる命令ニーモニックまたは演算コードを先ず定義する。第２に入力パラメータのセットがＣＦＡＰ３４からＣＦ３０にパスされる。第３に出力パラメータのセットがＣＦ３０によりＣＦＡＰ３４にリターンされる。命令処理装置１４２は暗号マイクロ命令記憶装置１４４に記憶されたマイクロ命令として具象化された暗号処理ステップの命令の特定順序を実施することにより選択された命令を実行する。制御流れおよび暗号処理ステップのそれに続く出力は入力パラメータの値とＣＦ環境記憶装置１４６の内容により決る。ＣＦ環境記憶装置１４６は例えば、キー，フラグ，カウンタ，ＣＦコンフィギュレーションデータ等のＣＦ３０内に収集的に記憶される暗号変数のセットからなる。記憶装置１４６のＣＦ環境変数はインタフェース３１を通して初期化されるが、それは入力パラメータを読みとり、ＣＦ環境記憶装置１４６にロードする、あるＣＦマイクロ命令の実行による。代りに、初期化はオプションの物理的インタフェースを通して行うこともできるが、これは暗号変数を例えば付属キー入力装置を通す等、直接にＣＦ環境記憶装置にロードすることができる。

【００２９】暗号化機構機密保護範囲１４０の物理的実施例では次の物理的安全保護の特徴を備えている。物理的実施例は暗号化機構３０へのアクセスを制限したインサイダアドバーサリによるプロービングに抵抗する。術語「制限した」というのは日，週でなく分，時間単位で測定される。アドバーサリ（敵）とは、高度の電子，機械設備を用いてアドバーサリの管理区域で発射される試験的攻撃と違い、制限された電子装置を用いてカストマーの場所でのプロービング攻撃に限定される。物理的実施例はまた各種の電気機械式検知装置を用いて物理的プロービングまたはイントルージョンでの試みも検出する。またこの暗号化機構３０の物理的実施例ではすべての内部に記憶された機密暗号変数のゼロ化を規定している。試みのプロービングまたはイントルージョンが検知されることがあると、自動的にこのゼロ化が行われる。物理的実施例はまた内部に記憶されている機密暗号変数のゼロ化に対する手動機能も備えている。前に引用したＡｂｒａｈａｍ等の特許出願を参照すると、如何にしてこういった物理的機密保護の特徴を実行できるかの例が示されている。

【００３０】キー生成プロセス：図６はこゝで開示する本発明の暗号化機構３０に含まれる暗号アルゴリズム１４４を説明するブロック図である。図６を参照し、暗号アルゴリズム１４４には暗号化および解読演算を行う暗号アルゴリズム１５０、キー作成用にキー生成アルゴリズム（ＫＧＡ）１５１および乱数作成用に乱数生成アルゴリズム１５２が含まれる。当面は乱数と擬似乱数とを区別しないこととする。すなわち乱数生成アルゴリズム１５２は真の乱数発生器でも、または擬似乱数を作成するアルゴリズムであっても良い。乱数発生器と擬似乱数発生器については以下に論ずる。暗号アルゴリズム１５０はデータ暗号化アルゴリズム（米国標準規格Ｘ３．９２－１９８１，データ暗号化アルゴリズム，米国規格協会，ＮｅｗＹｏｒｋ（１９８１年１２月３１日））等の対称アルゴリズムであってもよく、ＲＳＡアルゴリズムのような非対称、または公用キー，アルゴリズムであってもよい。公用キーアルゴリズムに対し、暗号化と解読との数学的演算間に差があってもなくてもよい。例えばＲＳＡアルゴリズムでは暗号化も解読も共にべき乗演算モジュロとして実行される。暗号アルゴリズム１５０にはインタフェース１５３を通し命令処理装置１４２がアクセスし、このインタフェース１５３が命令処理装置１４２に暗号化および解読の基本演算を行わせている。インタフェース１５３は同時にキー，データ，その他の暗号変数が暗号アルゴリズム１５０と命令処理装置１４２との間を通るようにしている。同様の方法で、キー生成アルゴリズム１５１には命令処理装置１４２がインタフェース１５４を通してアクセスし、インタフェース１５４は命令処理装置１４２にキー作成を要求させる。インタフェース１５４は同時にキー，データ，その他の暗号変数が２つの各構成品間にパスされるようにする。キー生成アルゴリズムはまた乱数生成アルゴリズムにインタフェース１５５を通してアクセスされる。これによりキー生成アルゴリズム１５１は、キー生成プロセスに必要な乱数生成アルゴリズム１５２からの乱数の要求，受理を行なう。乱数生成アルゴリズム１５２はまた命令処理装置１４２にインタフェース１５６を通してインタフェースをとり、命令処理装置１４２にキー作成以外の暗号化の目的に必要な乱数の作成を要求させる。

【００３１】暗号アルゴリズム１５０がＤＥＡのような対称または公用キー暗号アルゴリズムである場合は、キー生成アルゴリズム１５１によるキーの生成ステップは単純である。一般に、ｎビットキー（仮にｎ＝６４とする）で生成するプロセスは次のステップから成る。６４ビット乱数ＲＮが乱数生成アルゴリズム１５２から要求される。ある場合には、ＲＮは生成予定キーとして直接とられてもよい。しかし多くの暗号システムでは、キー生成には奇数パリティに対しキーの各パイトを調整するステップをも含んでいる。さらに他の場合では、キー値がある知覚された望ましくない性質を有さない，例えばキーが「実行時」あるいは「半実行時」ＤＥＡキーでないことを確めるため、キー生成アルゴリズムがキー値をテストすることがある。「実行時」または「半実行時」ＤＥＡキーの規格に関しては、ＭｅｙｅｒおよびＭａｔｙａｓ共著，「暗号－コンピュータデータ保護の新次元」Ｊｏｈｎ Ｗｉｌｅｙ ＆ Ｓｏｎｓ社、ＮｅｗＹｏｒｋ，１９８２年を参照のこと。キーのパリティを

調節することは多くの暗号システムで共通の慣行であるが、大抵の場合、この追加テストは無視される。

【００３２】暗号アルゴリズム１５０がＲＳＡアルゴリズム等の対象または公用キー暗号アルゴリズムの場合、キー生成アルゴリズム１５１でもってキーを生成するステップがより多く含まれる。公用キー暗号システムでは、公用キーおよび私用キーペア（ＰＵ１，ＰＲ１），（ＰＵ２，ＰＲ２）等は特殊キー生成アルゴリズム（ＫＧＡ）の助けをかりて作成される。ＫＧＡには、時にはＫＧＡがその暗号キーの作成に用いる乱数の作成をＫＧＡが作成または要求するプロセスの組合せを含んでいる。これら乱数はテストされ拒否されることがあり、他の乱数がある数学特性が満足されるまで要求されテストされることもある。さらに別の場合には、ＫＧＡがある乱数、またはある数学的特性あるいは複数の特性に対しテストされた後に受け付けた乱数値をとることがあり、この乱数値からその後１個以上の他の値を導出するであろう。一般に、ＫＧＡはキーの作成においてある単数および複数の乱数構成要素（すなわち乱数）を要求する。さもなければ、ＫＧＡが呼び出される度に同一の公用キーおよび私用キーペアが生成される恐れがある。この様なことは勿論許容されることでなく可能なキーペアのスペースから無作為に抽出され、または少く共無作為に抽出されているように思われ、従って敵がＫＧＡが作成したキーペアを推測する手段がないことを保証するような公用キーおよび私用キーペア（ＰＵ１，ＰＲ１），（ＰＵ２，ＰＲ２）をＫＧＡは作成しなければならない。上記のように、キーの作成において乱数を利用することに加え、ＫＧＡは数学的プロセスの使用を行い、このプロセスでは値ｔは他の値（すなわち、構成のプロセスの使用）から計算または導出され、試行錯誤のプロセスを用いて値を計算する（すなわち、所要の値が見つかる迄試行値をテストし拒否する）。好ましい実施例ではキー生成アルゴリズム中で直接シード値を用いるよりも擬似乱数発生器を初期化するのにシード値を用いている。その理由はシード値が必然的に、キー生成アルゴリズムがシードにおけるより多くのランダムビットを必要とするであろうという非ゼロ確率が存在していることを意味する特定有限長であるのに対し、擬似乱数発生器はキー生成アルゴリズムが必要とするだけ、任意長の擬似乱数を生成することが可能だからである。もしキー生成アルゴリズムがシードよりも多くのランダムビットを要するようなことが起れば、シード値の直接再使用は許容されないことになるであろう。その理由は、キー生成アルゴリズムはすべてのテスト基準を満足する出力への値を見出せないことがあるので、計算を完了できないことがあるからである。動的にシードされる擬似乱数生成アルゴリズムを使用すると擬似ビットの任意数の使用可能性を保証することにより、この潜在的無限くり返しは避けられる。

【００３３】図７は暗号アルゴリズム１５０がＲＳＡアルゴリズムである時のキー生成アルゴリズム１５１を説明する流れ図である。キー生成アルゴリズム１５１は公用キーおよび私用キーペアＰＵ＝（ｅ，ｎ）およびＰＲ＝（ｄ，ｎ）を作成する。こゝでｅ，ｄは公用および私用指数（ｅ，ｄはｎより小の正の整数）と呼ばれ、ｎは公用モジュラスである。従って２個組（ｄ，ｎ）において、私用指数ｄのみが機密保護を必要とする。図７を参照し、ステップ１６１でｐの試行値が生成される。ステップ１６２で、ｐの値が素数性に対しテストされる。素数性テストの方法を以下に述べる。ｐが素数ならば、制御はステップ１６３に進む。そうでなければ制御はステップ１６１に戻る（すなわち新ｐが生成される）。ステップ１６３でｐが「強」素数であるかどうかを調べるテストが行われる。「強」素数とは、選定したｐが素数ｐ，ｑにモジュラスｎを因数分解することにより暗号アルゴリズムを「ブレーク」するための数学的解析を許可しないことを保証する追加基準集合を満足する素数ｐを表わす本手法での術語である。キー生成およびｐ，ｑが暗号攻撃を妨げるのに充分強であることを保証するためにｐ，ｑについて実施される追加テストの論議に対しては、Ｒｉｖｅｓｔ，Ｒ．Ｌ、Ｓｈａｍｉｒ，Ａ．、Ａｄｌｅｍａｎ，Ｌ．「デジタルシグニチャおよび公用キー機密システムを得る方法」を参照のこと。ステップ１６３でｐについて実施される追加テストには、ｐ－１が大素数因数ｐ′を有することおよびｐ′－１が大素数因数ｐ″を有することのテストが含まれる。ＲＳＡキー生成について述べている文献で示唆されるその他のテストとしてｐ＋１が大素数因数を有することをテストするものもある。ｐが「強」素数ならば制御はステップ１６４に進み、その他の時は制御はステップ１６１に戻る。（すなわち新しいｐが生成される）。ステップ１６４でｑの試行値が生成される。ステップ１６５ではｐの値が素数性についてテストされる。ｐが素数なら、制御はステップ１６６に進み、その他の時はステップ１６４に戻る（すなわち新しいｑが生成される）。ステップ１６６でｑが「強」素数かどうかがテストされる。ステップ１６６でｑに実施される追加テストにはｑ－１が大素数因数ｑ′を有することおよびｑ′－１が大素数因数ｑ″を有することのテストを含む。ＲＳＡキー生成を論ずる文献が示唆する別のテストはｑ＋１が大素数因数を有することをテストすることである。もしｑが「強」素数ならば、制御はステップ１６７に進み、その他の時は制御はステップ１６４に戻る。（すなわち新しいｑが生成される）。ステップ１６７で公用モジュラスｎはｐとｑの乗算積として形成される。ステップ１６８で、値ｒは（ｐ－１）と（ｑ－１）の乗算積として構成される。ステップ１６９で、キー生成アルゴリズムにより、公用指数ｅが入力として与えられているかどうかが決定される。もし入力として与えられるならば、その時には制御はステ

ップ１７２に進み、与えられた値ｅがステップ１７１でテストされた条件を満たすと仮定される。別の実施例としては、制御がステップ１７１にフローすることができ、与えられた値ｅをキー生成アルゴリズム１５１によりチェックすることもできる。もし入力として与えられなければ、制御はステップ１７０に進み、ステップ１７０でｅの試行値を生成する。ステップ１７１でｅがｒに対し相対的に素であることを確認するためのテストを行なう。これは容易に実行され、ｅとｒの最大公約数（ＧＣＤ）が１であること、すなわちｅとｒが１以外の共通因数を有しないことをチェックする。ｅとｒが互いに相対的に素であれば、その時は制御はステップ１７２に進み、その他の時は制御はステップ１７０に戻る。（すなわち新しいｅが生成される。）ステップ１７２で、値ｄはｅとｄとの積が１モジュロｒと合同であるように計算される。ステップ１７３でＰＵ＝（ｅ，ｎ）とＰＲ＝（ｄ，ｎ）の計算値が出力としてリターンする。

【００３４】素数性に対し多数をテストする適切な手法の１つに、Ｒ．Ｓｏｌｏｖａｙ，Ｖ．Ｓｔｒａｓｓｅｎが「素数性に関する高速モンテカルロテスト」ＳＩＡＭ Ｊｏｕｒｎａｌ ｏｎ Ｃｏｍｐｕｔｉｎｇ，１９７７年３月，ページ８４，８５で述べた有効な「蓋然論（probabilistic）」アルゴリズムの使用がある。そこでは乱数「ａ」を一様分布（１，２，…，Ｘ－１）からとり、「ａ」の最大公約数およびＸが１であるかどうか、すなわちＧＣＤ（ａ，Ｘ）＝１をチェックし、またＪ（ａ，Ｘ）で表わす「ａ」とＸのヤコビの記号がＱモジュロＸに合同かどうか（ただしＱは「ａ」の(X-1)／２べき乗に等しい）をテストする。こゝで整数（ａ１，ａ２，等）の集合（但し集合中の各「ａ」はＸより小さい）を用いてＸを素数性に関してテストする。図７に示すように、ＲＳＡキーを生成する場合には値Ｘを値ｐ，ｑに置き換えることに注意する必要がある。このテストでは、セット中の各「ａ」の値に対し、上記の両条件が保持されることが必要である。従って集合中に両条件が保持されない「ａ」があれば、Ｘは複素数であることが分かる。その他の時はＸは素数として受容される。この手順は選択した数が素数であることを保証するのではなく、素数性のテストに失敗しなかったことのみを保証している。集合中の整数ａ（ａ１，ａ２等）の数が大きい程、選択した数が素数である確率が大きい。たゞし勿論集合中の各整数「ａ」に対し両条件が満足されていることが仮定されている。２整数の最大公約数、２整数の最小公倍数、２整数のヤコビの記号の計算法は技術上周知である。

【００３５】適切な暗号保護を達成するＲＳＡアルゴリズムに対し、モジュラスｎがほぼ５１２ビットと１０２４ビット間の数であることが必要なことは当業者によく知っている。前記のキー生成アルゴリズムでは、公用キー指数ｅはキー生成アルゴリズムに規定することも、キー生成アルゴリズムにより生成することも可能である。ｅをキー生成アルゴリズムに規定する利点は小さな値（例えばｅ＝３）を規定できることである。公用キーで暗号化する時はこれにより性能が向上する。私用指数ｄは従属変数であり、導出されなければならない。従って実用上は、ｄはモジュラスと同一サイズになる。この場合モジュラスが５１２ビットなら、選択した指数ｅのビット数により、公用キーＰＵは５１４ビット～１０２４ビットであり、他方私用キーＰＲは１０２４ビットである。６４ビットまたは１２８ビットのＤＥＡと比べると、ＲＳＡキーはかなり大きい。当業者には公用キーアルゴリズムが可成り計算的に強力な手順であることも認められる。単一の公用キーおよび私用キーペアを生成するのに必要な時間で、数千、恐らく数百万ものＤＥＡキーを生成できる。固定ブロックサイズのＤＥＡと違って、ＲＳＡアルゴリズムは特定のブロックサイズを要しない。そのために選択したモジュラス長により、ＲＳＡキー生成が比較的短かったりまたは比較的長いプロセスであったりすることができる。キー生成アルゴリズム１５１が希望サイズ（すなわち規定ビット数）の公用キーおよび私用キーを生成するために、生成されたｐとｑが共に掛け合わせると希望のサイズ、あるいはビット長のモジュラスｎを生ずるようにステップ１６１と１６４とを設計する。ｐ，ｑに関する追加テストを図７の流れ図に追加でき、これによりＩＳＯ Ｄｒａｆｔ Ｉｎｔｅｒｎａｌ Ｓｔａｎｄａｒｄ ９７９６「メッセージ回復を与えるデジタル署名計画」のような暗号規格中で規定されることのある仕様に従って、キー生成を適合させ得ることに当業者は理解するであろう。また図７に述べたＲＳＡキー生成アルゴリズムは、ｐとｑの作成が単に試行錯誤法ではなく、試行錯誤とその値を構成する方法とを組合せるプロセスで行うならば、より効率が上るということを当業者は認めるであろう。ｐの生成、ｐ－１が大素数ｐ′を有することのテスト、ｐ′－１が大素数ｐ″を有することのテストの代りに、大素数ｐ″を生成することから開始することも出来る。この場合、少数をｐ″に乗じ、１を加え、次にプライマリティのテストをすることによりｐ″から素数ｐ′を見つける。この結果得られたｐ′が素数でなければ、ｐ″に別の少数を乗ずる以外は同じプロセスを繰り返す。同じ手法でｐ′からｐも見出すことができる。同様に、同じ手法を使ってｑ″からｑを見出すことができる。

【００３６】ＲＳＡキー生成には多くの変形がありうることを当業者は認めるであろう。しかしどんな場合にも、キー生成プロセスでは乱数が必要であり、この乱数は乱数発生器または擬似乱数発生器を用いて作成することが出来る。図７に戻ると、ステップ１６１，１６４ではｐ，ｑの試行値が無作為に生成される。一度生成されると最も重要性の少ない（低位または右端）ビットをＢ「１」に等しく設定することができ、生成値が必ず整奇

数であることが確実となる。値２を除きすべての素数は奇数であるから、これにより処理が速くなる。上述のようにｐとｑをｐ″とｑ″とから生成する場合は、ｐ″とｑ″の試行値を無作為に生成する。公用指数ｅがキー生成アルゴリズム１５１に入力として与えられていない時には、ｅの試行値を無作為に生成する。このようにして、すべての場合に、ＲＳＡキー生成には乱数の作成と使用の必要なことが分る。

【００３７】乱数および擬似乱数：大抵の暗号システムでは乱数を作成、使用する手段が必要である。例えば、ＤＥＡによる暗号化の暗号ブロック連鎖モードを使用する時など、乱数を初期化ベクトルまたは初期連鎖値として使用する。例えば、ＤＥＡによる暗号化の暗号フィードバックモードを使用する時などは、乱数を「シード」値として使用する。多くの暗号ベース識別および認証プロトコルでは乱数をその場限りに使用する。乱数作成能力がないと、大抵の暗号システムは著しく制約を受けるかまたは使いものにならないであろう。

【００３８】図８および図９に暗号システムで乱数を生成するのによく用いられる２方法を示す。図８は「真」乱数発生器１８０のブロック図である。「真」乱数発生器１８０にはハードウェア回路１８１を含み、乱数を作成する能力がある。かゝるハードウェア発生器で乱数を作成する手段はよく知られており従来技術で実行できる（前記ＵＳＰ４，９０５，１７６，Ｒ．Ｓｃｈｕｌｚ「乱数発生器回路」１９９０年２月２７日発行を参照）。乱数の要求はインタフェース１８２を通して入力される。生成された乱数（ＲＮ１，ＲＮ２等）はインタフェース１８３を通し出力される。実際には生成された乱数の長さはアルゴリズムの固定定数例えば６４ビットである。「真」乱数発生器はその出力値が予想不能であるという性質を有する。すなわち乱数発生器の出力を予測するようなアルゴリズムを構成する筈はない。「真」乱数発生器は初期化にシード値を必要とせず、従って発生器の出力を繰り返させる方法は存在しない。この性質が「真」乱数発生器を暗号システムでの実行を非常に望ましいものにしている。しかし「真」乱数発生器のコストは擬似乱数発生器に比べて比較的高いため、大抵の商用暗号システムは擬似乱数発生器を使用している。

【００３９】図９は初期にシードされる擬似乱数発生器１９０のブロック図である。初期にシードされる擬似乱数発生器１９０にはアルゴリズム１９１および乱数生成にアルゴリズム１９１が使用するシード値記憶のためのシード記憶装置１９４を有する。（擬似乱数発生器により作成された乱数は一見無作為に見えるだけであることに注意を要する。より正確には、擬似乱数発生器により作成される出力は擬似乱数と呼ぶべきである。しかし便宜上これらも乱数と呼ぶことにする）。初期シード値はインタフェース１９５を通し指定される。初期シード値自体は暗号命令の１つを通し暗号機構にインタフェースするユーティリティプログラムを通し暗号システムに入力されるか、または入力されたパスワードあるいは物理的なキー操作スイッチを用いて許可されたインストレーション要員のみが操作できる特殊前面パネルインタフェースを通し入力される。キー生成に擬似乱数発生器を使用する場合は、初期およびその後すべてのシード値は機密にしておかなければならない。そうでなければ、擬似乱数発生アルゴリズムは公用領域にあると考えられるから、生成された乱数の機密度はシード値を秘密にしておくことに依存している。乱数を生成する時には、シード値はアルゴリズム１９１の性質にもよるが、アルゴリズム１９１により動的に更新されることがある。アルゴリズム１９１にはまた、乱数作成中自動的に更新されるカウンタ数またはシーケンス数の記憶装置のような、別個の記憶装置を有するものがある。この場合には、シード値は一定のまゝでカウンタ数またはシーケンス数のみが更新される。カウンタ数またはシーケンス数を用いるケースでは、シード記憶装置１９４にシード値がインタフェース１９５を通して初期化される時に初期値がアルゴリズム１９１によりセットされる。乱数の要求はインタフェース１９２を通し入力される。生成された乱数（ＲＮ１，ＲＮ２等）はインタフェース１９３を通し出力される。実際には生成された乱数の長さはある固定値、例えば６４ビットである。擬似乱数発生器はその出力が完全に予想可能であるという性質を有す。擬似乱数発生器の出力は一見無作為に見える数値の列（ＲＮ１，ＲＮ２等）である。アルゴリズムがいわば「メモリ」を有している理由のみで、ＲＮ２はＲＮ１とは違っている。すなわち、アルゴリズムは連続的に自身を更新しており、アルゴリズムが呼び出される度に違った「出発」点から始まる。しかし、もし同じアルゴリズム１９１の各場合が同じシード値で初期化されたとしたら、各アルゴリズム１９１により作成される乱数は完全に同一となろう。初期シード値自体を無作為プロセスを通して選択すべきであるということが良い暗号実施法である。こうすると別々の暗号装置で各々初期にシードされる擬似乱数発生器１９０は異なる乱数を作成する。

【００４０】図１０は動的にシードされる擬似乱数発生器２００のブロック図である。動的にシードされる擬似乱数発生器２００は乱数発生用にアルゴリズム２０１を有する。乱数の要求はインタフェース２０２を通し入力される。生成された乱数（ＲＮ１，ＲＮ２等）はインタフェース２０３を通し出力される。インタフェース２０３で生成された乱数（ＲＮと名付ける）の長さはインタフェース２０２における長さパラメタにより規定される値に等しい。アルゴリズム２０１には内部に記憶されたシード値を有しない。その代り要求されるシード値はインタフェース２０２においてアルゴリズム２０１に指定される。このシード値は呼出し者に見えなければならないが、それは同一シードを入力すれば同一出力が生ずる

ことを保証しながら他の呼出し者による要求のインタリーブを行なえるからである。便宜上、長さ値が生成される乱数長を決める所では、アルゴリズム２０１では長さパラメタをインタフェース２０２で指定してよい。実際上は、シードの長さは大抵はアルゴリズム２０１が予め設定した固定定数である。動的にシードされる擬似乱数発生器２００の演算を説明するため次のことを仮定する。（１）パラメタ「長」はビットで指定され、（２）パラメタ「シード」のビットでの長さは１２８であり、Ｌは望ましい乱数（ＲＮと称する）のビットでの長さである。その場合パラメタ「長」で指定される値は１２８＋Ｌ、すなわち次期シードの長さプラス望ましい乱数の長さで計算される。

【００４１】別の実施例では、次期シードの作成を自動的に行うと、従ってパラメタ「長」は望ましい乱数ＲＮの長さを指定することになる。その場合は、インタフェース２０３では２つの出力、次のシードとＲＮがある。いずれの実施例も作動する。最初の場合では、動的にシードされる擬似乱数発生器２００は次期シードを作成する方法については意識しない。次期シード値の作成、管理は呼出し者の制御下にある。第２の場合では、動的にシードされる擬似乱数発生器２００は呼出し者に次期シード値を計算して戻す責任がある。

【００４２】さらに別の代替実施例では、初期にシードされる擬似乱数発生器のアルゴリズムと動的にシードされる擬似乱数発生器のアルゴリズムとが同じアルゴリズムであり、アルゴリズムには同一の回路および／またはルーチンを用いることができる。初期にシードされる発生器は普通のユーザではアクセスできないシステム記憶装置を用いていてシステムシード値を有し、これは初期にシードされたアルゴリズムが呼出されると必要に応じて自動的に更新される。また動的にシードされる発生器は呼出し者にそのシード値をパス（および維持）するよう要求する。上記方法に対し小修正や変化を加えた多くの実施例が可能であり、この相異点は本発明に何等影響しないことを関係者は認めるであろう。

【００４３】本発明では、公用キーおよび私用キーペア（ＰＵ，ＰＲ）はユーザによる入力として機密パスフレーズから生成されており、その実行のためにはキー生成アルゴリズムが同じ順序の乱数を再生成するし、従って同じパスフレーズがキー生成アルゴリズムに指定される度に同じキーペア（ＰＵ，ＰＲ）を再生成することが出来ることが極めて重要である。これと対照的に、暗号システムで乱数を要求する他の暗号アプリケーションは全て、同じ順序の乱数を再生成する必要を有しない。実際には、かゝる能力が暗号システムに存在するとキーが偶然再生成されるような好ましくない状態に通ずる可能性があると言われることもある。

【００４４】図８、および９に示す方法によりキー生成アルゴリズムが要求する乱数を作成する場合には、再生成従ってパスフレーズから公用キーおよび私用キーペア（ＰＵ，ＰＲ）を生成することは不可能である。図８の「真」乱数発生器１８０は、キーペア（ＰＵ，ＰＲ）を満足に再生成するために必要となる同一順序の乱数を再生成させる方法がないので、使用することが出来ない。同様に、図９の初期にシードされる擬似乱数発生器１９０も、同一順序の乱数を再生成せしめる方法を有しないので使用出来ない。実際には、暗号システムに電源が入りラインにつながった時、または時には装置の電源が切れていた期間の後で一度だけかゝる擬似乱数発生器が通常初期化される。その後は単に乱数を要求するだけでよい。すなわち動的にシード値を再指定する用意はない。多くの場合呼出し者は手許にシード値を有さないので、擬似乱数発生器の各呼出し者に彼自身の「シード」値の入力を要求するよりも、むしろ一度だけ擬似乱数発生器に「シード」する業務を行うのが最も良い。事実多くのシステムユーザが使用すると考えられるこの形式の擬似乱数発生器に、通常のユーザがシード値を指定できないということは機密保持の観点から重要である。

【００４５】以上の説明から図１０に図示する動的にシードされる擬似乱数発生器は、本発明の要求を満足できるが、大抵の暗号システムにおいては乱数作成の一般要求を満たさないことは明らかである。問様に前記の説明から、図８に示す「真」乱数発生器および図９に示す初期にシードされる擬似乱数発生器は大抵の暗号システムにおける乱数作成の一般要求を満足できるが、キー生成アルゴリズムがパスフレーズからキーを再生成しなければならない時の乱数作成の要求を満足しない。従って、本発明の好ましい実施例においては、図１１に示すように乱数生成用に２手段が必要とされる。図１１を参照すると、図６で前に図示した暗号化機構の暗号アルゴリズム１４４構成品は動的にシードされる擬似乱数発生器２００およびキー生成アルゴリズム１５１と動的にシードされる擬似乱数発生器２００間のインタフェース２０４を含むように拡張されており、乱数要求によりリターンすべき乱数を生成せしめる。図１１の動的にシードされる擬似乱数発生器２００は既に述べた図１０の動的にシードされる擬似乱数発生器２００と同一に作動すると仮定されている。すなわち、乱数要求には長さとシードの指定を含む。出力は乱数である。キー生成アルゴリズム１５１はシード値を管理すると仮定される。例えば第１シードはこれから述べる方法を用いてパスフレーズから計算する。キー生成アルゴリズム１５１が長さＬの乱数を要求する時はいつもＬ＋１２８の「長さ」パラメタを指定する。すなわち次期シードを自動的に要求し、キー生成アルゴリズム１５１にアクセスできる次期シード格納域に保管する（例えばキー生成アルゴリズム１５１内に）。図１１のキー生成アルゴリズムが図７のＲＳＡキー生成アルゴリズムそのものである場合には、図７のステップ１６１，１６４，１７０が図１１のインタフェー

ス２０４での動的にシードされる擬似乱数発生器２００に向けられる乱数の要求になるであろう。従って図７のステップ１６１，１６４または１７０が繰返される度に、新乱数が得られる。満足な値を見出すまでにどれだけの試行を必要とするかを予め知る方法はなく、プロセスは試行錯誤であるから、乱数の順序を予め計算出来ず必要の都度試行を行う。

【００４６】図１２は本発明の要求を満足する動的にシードされる擬似乱数発生器の例である。アルゴリズムは１２８ビットを要し、これを６４ビットキーＫと６４ビット初期連鎖値ＩＣＶとに分割する。シードの左側６４ビットがＫになり、シードの右側６４ビットがＩＣＶになる。ｍを発生する無作為ビットの数とすると、６４ｎにｍより大の最小値を表わさせる。こゝでｎはｍビットの擬似ランダムシーケンスを作成するのに充分の長さを有する生成すべき暗号文の６４ビットブロックの数を表わす。暗号文を生成するのに、２進ゼロのｎ６４ビットブロックでスタートし、ＤＥＡ暗号化の暗号ブロック連鎖モードを用いてＤＥＡアルゴリズムで暗号化する。キーと初期連鎖値は上記のＫとＩＣＶそのものである。長さｍの出力乱数ＲＮは結果の暗号文における左側（最も重要な）ｍビットそのものである。

【００４７】パスフレーズを使用するキー生成：図１３は暗号システムを図示しており、暗号化機構（ＣＦ）３０、暗号キーデータセット（ＣＫＤＳ）３２、暗号化機構アクセスプログラム（ＣＦＡＰ）３４およびアプリケーションプログラム（ＡＰＰＬ）３６を有する。こゝで図１３を参照すると公用キーおよび私用キーペア（ＰＵ，ＰＲ）を生成するステップをトレースできる。４０においてアプリケーションプログラムＡ（ＡＰＰＬＡ）４２がユーザにより呼び出される。ＡＰＰＬＡは（１）アプリケーションが処理とつながる以前にユーザが自分のキーを生成または再生成することを要求するアプリケーションであるか、または（２）ユーザがそれらのキーを生成または再生成することを許容するユーティティであることを仮定している。ＡＰＰＬ　Ａは、ユーザが４１で入力するパスフレーズ（ＰＰと称する）をユーザに催促する。応答して、ＡＰＰＬ　Ａは４３でキー生成機能４７をコールする。４３はＣＦＡＰ３４にあり、モードパラメータＰＰおよび制御情報をパスする。制御情報は制御ベクトルまたは制御ベクトルをつくるのに用いられる情報であってもよい。モードパラメータは生成キーがパスフレーズベース（モード＝「ＰＰ」）で生成されるか、されないか（モード＝「非ＰＰ」）いずれをキー生成機能に指示する。従ってＰＰパラメータは選択パラメータである。制御情報はキータイプ（すなわち生成すべき公用キーおよび私用キーのタイプ）およびキー管理でのキーの使用法を示す取扱い制御情報である。応答して、キー生成機能４７は（１）入力パラメータをパーズし、（２）もしモード＝「ＰＰ」なら入力パスフレーズＰＰから１２８ビットハッシュ値ＣＷを計算し、入力制御情報を処理し、ＧＲＶＰＲ命令を指定される制御データパラメータを作り、ＧＰＵＰＲ命令５２を呼び出して５０で暗号化機構３０の命令処理装置１４２で実行する。５０はモードパラメータおよびもしモード＝「ＰＰ」ならオプションコードワードＣＷ、および制御データをパスする。制御データには生成すべき公用キーＰＵと関係するキー関連情報を指定するＰＵ制御ベクトルおよび生成すべき私用キーＰＲに関連するキー関連情報を指定するＰＲ制御ベクトルを含む。各制御ベクトルには暗号システム内のキーを識別するキー名を含んでいる。各制御ベクトルは問時にラベルまたはＣＦにより初期化されるべきＣＫＤＳラベルの予約スペースを含み、暗号キーデータセット（ＣＫＤＳ）３２からのキートークンの記憶、検索に用いることができる。応答して、ＧＰＵＲ命令５２は、図１４に、より詳細な記述があるように、入力としてモードパラメータ、またもしモード＝「ＰＰ」ならコードワードＣＷをパスして、キー生成アルゴリズムＫＧＡを呼び出す。応答して、ＫＧＡは図１４に詳細記述があるように公用キーおよび私用キーＰＵ，ＰＲを生成し、ＧＰＵＰＲ命令５２にリターンする。応答して、ＧＰＵＰＲ命令５２は生成されたＰＵを含むＰＵキートークンおよび生成されたＰＲを含むＰＲキートークンをつくる。ＰＵキートークンおよびＰＲキートークンは図１５に説明されており、以下詳しく述べる。ＧＰＵＰＲ命令は以下詳細説明するように、同時に５０で入力としパスされるモードおよび制御データについて一貫性チェックを行う。一貫性チェックにより、キータイプと各キートークンの制御ベクトル部分の取扱い情報とがモードと一致していること、すなわちキーがパスフレーズから生成されたか否かが確められる。ＰＵ，ＰＲキートークンは次にキー生成機能４７に５１でリターンされる。応答して、キー生成機能４７は必要ならＰＵ，ＰＲキートークンを更新する。例えばＣＫＤＳラベルの記憶装置に対するトークンの予約フィールドがこの時点で埋められる。次にキー生成機能４７はキー記憶装置マネージャ４６にＣＫＤＳ３２の１個または２個のキートークンを記憶させ、４４でＡＰＰＬ　Ａにキー名またはラベルのみをリターンさせるか、または４４でＡＰＰＬ　Ａに１個または２個のキートークンをリターンする。こゝでの意図はＡＰＰＬ４２にキートークンを管理、制御させる（もしそう望むなら）か、暗号システムにキートークンを管理、制御させることである。どちらの進め方にも利点があり、キートークンがＣＫＤＳ３２に記憶されるにしても、あるいはＡＰＰＬ４２にリターンされるにせよ、キートークンの取扱いは４３でのキー生成機能４７へのＡＰＰＬ　Ａ４２により指定される入力パラメータの制御下にあるように暗号システムを設計することが可能である。応答して、ＡＰＰＬ　Ａは必要に応じキートークンを記憶するか、またはＣＦＡＰで

実行する他の暗号機能への入力として、ＰＵ，ＰＲキートークンが後で再指定できるキー名またはラベルを記憶する。こゝでＡＰＰＬ　Ａはユーザに、要求された公用キーおよび私用キーが入力パスフレーズから生成されたということを指示する。ＡＰＰＬ　Ａは処理が完了する時迄必要に応じ処理を続ける。生成したキートークンの１個以上がＣＫＤＳ３２に記憶されたと仮定すると、ＡＰＰＬ　Ａは４５でキーパージ機能４８をコールする。４５はＣＦＡＰ３４にあり、パージされるべき各キートークンのキー名またはラベルをパスする。応答して、キーパージ機能４８はキー記憶装置マネージャ４６にＣＫＤＳ３２から各キートークンを抹消させる。もしＡＰＰＬ　Ａがキートークンを管理しているなら、キーパージ機能４８をコールする代りに、ＡＰＰＬ　Ａがキートークンをパージする。図１３には示されていないが、各呼出しエンティティには適当なリターンコードおよび条件コードを利用できると仮定されており、従って要求された処理が正常に完了したこと、あるいは追加の処置を要するエラーが発生したかどうかの指示を呼出しエンティティは有している。キー生成機能４７およびＧＰＵＰＲ命令５２は次の２タイプのキー生成を操作するように設計されていることを当業者なら認識できる。（１）ＰＵ，ＰＲがパスフレーズから生成される場合（モード＝「ＰＰ」）、（２）ＰＵ，ＰＲがパスフレーズから生成されない場合（モード＝「非ＰＰ」）。すなわち、キー生成機能およびＧＰＵＲ命令の設計は本発明の好ましい実施例であると考えていることをベースにしている。その理由は、いずれのモードとも両方の種類のキー生成を行うことは出来ず、また各モードは今論じた通りキー管理においてそれぞれ独自の異なる利点を有するからである。

【００４８】公用キーおよび私用キーペア（ＰＵ，ＰＲ）が生成される時、このキーがパスフレーズから生成されたものであるか否かを識別することが重要である。基本的にはパスフレーズから生成されたキーはユーザに知れるキーである。直接には知れなくとも、このキーはユーザが計算でき、従って厳密な意味ではユーザに知られる。これはＰＵ，ＰＲの計算に用いられるアルゴリズムは公用領域にあると推定されるからである。すなわち機密が保たれる根拠がない。唯一の機密要素はパスフレーズその物である。従って、パスフレーズを知る人はキーを知る（または計算する）ことができる。しかし公用キーおよび私用キーペア（ＰＵ，ＰＲ）がパスフレーズから生成されない時、すなわちキー生成プロセスに含まれる無作為要素または無作為値が真の乱数発生器（図８）か、初期にシードされる擬似乱数発生器（図９）のいずれかを用いて暗号機構で生成される時は、キー生成アルゴリズムにより生成されるキーはすべての実用目的に対してはユーザには知られないかまたは知ることができないものである。（多くの場合、キーはマスタキーの下で暗号化されており、生成されるキーはマスタキーと同程度の機密度を有す。マスタキーを知る人は誰でも生成されるＰＵとＰＲも知ることになるが、ＰＵは公用キーであるから懸念する要はない。）「スマート」キー管理設計では、両タイプの生成キーを利用することができる。パスフレーズから生成されない私用キーＰＲは、理論上は暗号システム自体によってのみ知ることが出来る。従って適正に実行するなら、完全性のシステムレベルあるいは機密性のシステムレベルの実行にこういったキーを用いることができる。これはＰＲがユーザに知られるなら ば達成されないものである。反面ユーザに知られるＰＲにより、よく利用される多くの機能がある。例えば、暗号システム自体にそのユーザを認証する、またはそのユーザを他のユーザに認証する、または情報をそのユーザから来ていると認証する（例えば、ユーザが計算して彼のメッセージにディジタル署名を添付する場合）のにＰＲは使用される。キー管理設計は次の方法でこの差を利用することがある。ＧＰＵＰＲ命令５２の処理の一部として、ＰＵ，ＰＲキートークンを作るステップがある。

【００４９】図１５にＰＵキートークンおよびＰＲキートークンの書式を示す。ＰＵキーは公用キーであるから、ＰＵキートークンはクリアまたは暗号化されたフォームｅＫＭ．Ｈ１（ＰＵ）でＰＵを記憶することがある。こゝでＫＭ．Ｈ１はＣＦ３０のＣＦ環境記憶装置１４６内に記憶されている機密マスタキーＫＭと暗号変数Ｈ１との排他的論理和積であり、Ｈ１は中間ハッシュ値１を作成するのにＣ１をハッシュし、またＨ１を作成するのにハッシュ１に数ビットをフィックスすることによりＰＵに対し制御ベクトルから作成される。ｅＫＭ．Ｈ１（ＰＵ）の正確な規格は前記のＳ．Ｍ．Ｍａｔｙａｓ等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムキー管理」に述べられている。ＰＲキーは私用キーであるから、ＰＲキートークンは暗号化したフォームｅＫＭ．Ｈ２（ＰＲ）でのみＰＲを記憶する。ｅＫＭ．Ｈ２（ＰＲ）の正確な規格は前記のＳ．Ｍ．Ｍａｔｙａｓ等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムのキー管理」に述べられている。ＰＵとＰＲを暗号化する暗号化変数Ｈ１とＨ２は異なっている。Ｈ１は公用キーＰＵに関連する制御ベクトルＣ１より導出し、Ｈ２は私用キーＰＲに関連する制御ベクトルＣ２より導出する。ＰＵ，ＰＲキートークンは、それぞれキー名またはＣＫＤＳラベル、使用法制御情報等のキー関連データである制御ベクトルＣ１，Ｃ２も含む。ＰＵ，ＰＲキートークンにはまたフォームｅＫＭ．Ｈ１′（ＫＡＲ）、ｅＫＭ．Ｈ２′（ＫＡＲ）の確証を含んでいる。たゞしＣＫＡＲはキー確証レコードであり、Ｈ１′，Ｈ２′はＨ１，Ｈ２に係わる暗号化変数である。ＫＡＲはクリアまたは暗号化キーすなわちＰＵ，ｅＫＭ．Ｃ（ＰＵ）またはｅＫＭ．Ｃ（Ｐ

Ｒ）の暗号機能である。ｅＫＭ．Ｈ１′（ＫＡＲ）およびｅＫＭ．Ｈ２′（ＫＡＲ）の正確な規格は前記のＳ．Ｍ．Ｍａｔｙａｓ等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムのキー管理」に述べられている。ＰＵ，ＰＲキートークンにはキートークン中に他のフィールドの記憶位置と長さを識別する情報を有するヘッダ部分も含んでいる。これによりそのフィールドを可変長にすることができる。

【００５０】図１６にはＰＵ、ＰＲキートークンの制御ベクトル部分の追加規格を示す。図１６を参照すると、制御ベクトルにはＣＶタイプと名付ける制御ベクトルタイプフィールドを含んでおり、キーが公用キーか私用キーか、さらにそのキーはユーザキーか、キー管理キーか、証明キーか、あるいは認証キーを示す。４つのキータイプ（ユーザ、キー管理、証明、認証）の正確な識別は本発明では重要ではない。しかし、異なるキータイプはキー管理設計において異なる目的と用途を有することを理解するのは重要である。例えば、タイプ＝「ユーザ」と制限して、公用ユーザキーがディジタル署名を生成するためのみに用いられることができる。他方タイプ＝「キー管理」はより広範であり、私用キー管理キーを暗号化の目的に、またある暗号装置から他の暗号装置にＤＥＡキーを分散する目的に使用することも、また公用キー管理キーにディジタル署名を生成させることも可能である。例えば、公用キー、私用キーペアはキーを暗号化するＤＥＡキーを分散するために２つの暗号システム間で用いることができる。その後は、キーを暗号化するキーは他をＤＥＡキーを２つの夫々の暗号システム、例えばデータキー間に分散するのに用いられる。この場合は、一般にはこの目的に公用ユーザキー、私用ユーザキーを用いようとはしないであろう。その理由は、この場合は、自分の私用ユーザキーを知っているか、または理論的に知りうるユーザ自身はキーを暗号化する暗号化されたキーをインタセプトし（すなわち、ＰＵで暗号化されたキーを暗号化するキー）、またそれを自分の私用キーＰＲで解読することができるからである。このようにして、ユーザはキーを暗号化するクリアキーの値を見出すことが可能であり、たいていの暗号システムではキー分配プロトコルの所期の機密保護に打ち勝つことになる。従って、ＰＵ、ＰＲキートークンをＧＰＵＰＲ命令５２が作る時点において、生成されたキーのキータイプおよび使用法が意図されたキー管理設計に合致することを確認するため５０での入力として指定されたモードに対し、図１４の５０での入力として指定されたＰＵ、ＰＲ制御ベクトル（または等価的には図１３の５０での制御データ）に関する一貫性チェックをＧＰＵＰＲ命令が実行しなければならないことは本発明の一部である。例えばＣＦＡＰがモード＝「ＰＰ」を指定し、制御データがタイプ＝「キー管理」を指示するならば、その時はＧＰＵＰＲ命令５２はこの不一致を検出し、キータイプに対する不一致指示により処理を停止したというＣＦＡＰへの指示でもって演算を打ち切らなければならない。他方では、もしＣＦＡＰがモード＝「ＰＰ」を指定し、制御データがタイプ＝「ユーザ」を指示するならば、その時はＧＰＵＰＲ命令５２はキータイプの不一致により演算を打ち切ってはならない。ここでは述べないが、追加の一貫性チェックがＧＰＵＰＲ命令に演算を打ち切りうることがあることに注意を要する。キートークンに生成されたキーがキータイプおよび使用法を指定する制御情報に連結されることは重要であるから、本発明の好ましい実施例では図１５のＰＵキートークンは、暗号化された書式ｅＫＭ、Ｈ１（ＰＵ）でＰＵを記憶しなければならない。前記のように、Ｈ１をキートークンの制御ベクトルに従属させることにより、これが達成される。Ｈ１を制御ベクトルに従属させる正確な方法はここでは重要でないが、前記のS.M. Matyas 等による同時係属特許出願「制御ベクトルを用いる公用キー暗号システムのキー管理」に詳細が述べられている。前述から、本発明はユーザ供給のパスフレーズから公用キーおよび私用キーペアを生成する手段を提供することは理解されるであろう。しかし大抵の暗号システムでは、上記のようにユーザが私用キーＰＲの値を予測したり、決定する能力を有さないような方法で、公用キーおよび私用キーを暗号システム内で生成する時には、より機密保護された設計が可能である。従って本発明では、キーペアがパスフレーズから導出されたか、またはキーペアがパスフレーズから導出されていないかによって、生成されるキーのタイプの双方の使用法を制御する手段も提供するものである。従来技術（ＵＳＰ４，９４１，１７６，４，９１８，７２８，４，９２４，５１４，４，９２４，５１５，５，００７，０８９）では制御ベクトルを通してキータイプおよびキー使用法を制御する手段が述べられている。しかし、この従来技術は、キーが如何にして生成されるかに従ってキーのタイプと使用法を制限する方法は述べていない。対照的に、本発明は公用キーおよび私用キーがパスフレーズから生成されるキーと、パスフレーズから生成されていないキーとを区別し、指定されるキータイプが許可さるべきか、または許可さるべきではないかをキー生成命令（すなわちＧＰＵＰＲ命令）内で決定する手段として、この区分がキー管理に重要であることを示した。このようにして本発明は生成プロセスを適当に制御する手段を提供し、そのため生成されるキーは、キーのタイプおよびそれが暗号システム内で如何に処理されるかを指定する制御ベクトル情報に、適当に暗号的に連結されることになる。生成されるキーを制御するこういった手段がなければ、パスフレーズおよびパスフレーズから生成されるキーの利点は暗号システムの全体機密保護を弱めるように思われ、パスフレーズから導出するキーの利点は利点ではなく欠点となるように思われることになろう。従って、本発明は単にパスフレーズ

からキーを生成する手段を提供するのみではなく、キー管理内で生成されたキーを制御する本質的な手段をも提供するものである。

【００５１】図１４は、ＧＰＵＰＲ命令５２を呼び出す結果としてＣＦ３０内で実行される演算の説明である。図１４のＧＰＵＰＲ命令５２は、図１３のＧＰＵＰＲ命令５２とは、図１４がキー生成アルゴリズム１５２および動的にシードされる擬似乱数発生器２００を呼び出す追加のステップがあるという点以外は全く同一である。図１４を参照すると、５０での入力はモード、オプション命令語（ＣＷと呼ぶ）、ＰＵ制御ベクトル、ＰＲ制御ベクトルよりなる。図１３では、ＰＵ制御ベクトルおよびＰＲ制御ベクトルは単に制御ベクトルと呼ばれている。呼び出されたことに応答して、ＧＰＵＰＲ命令５２は５３でキー生成アルゴリズムＫＧＡ１５２を呼び出し、モードパラメータおよびオプションＣＷをパスする。応答して、ＫＧＡ１５２はキー生成を実行するステップを遂行する。例えば、ＣＦ３内で行われる暗号アルゴリズムがＲＳＡアルゴリズムならば、その時にはキー生成ステップは図７に示す通りのものである。ＫＧＡ１５２が乱数を要求する最初の時に、ＣＷの値が初期シードとして用いられ、パラメータ「長さ」の値を得るために要求される乱数ＲＮの長さが値１２８に加算される（これが次期シードの長さになる）。

【００５２】次にＫＧＡ１５２は５５で動的にシードされる擬似乱数発生器２００を呼び出し、「長さ」とシードＣＷを入力パラメータとしてパスする。応答して、動的にシードされる擬似乱数発生器２００はＣＷに等しい入力シードから「長さ」に等しい長さの乱数を生成する。例えば、図１２に示すアルゴリズムを動的にシードされる擬似乱数発生器２００として用いることができる。「長さ」に等しい長さの生成された乱数ＲＮは５６でＫＧＡ１５２にリターンされる。図１４は次期シードおよびＲＮとして５６での出力を示す。実際には、生成される乱数ＲＮは（長さ１２８ビットの）次期シードおよびＲＮ（「長さ」に等しい長さマイナス１２８ビットの望ましい乱数）の単なる連結である。ＲＮを受理すると、ＫＧＡ１５２は次期シードおよびＲＮを得るためそれをパーズする。ＫＧＡ１５２が動的にシードされる擬似乱数発生器２００に別のコールをすることが必要と判断した場合は、次期シード値はセーブされる。次にＲＮ値がキー生成プロセスで用いられる。次回ＫＧＡ１５２が乱数を要求する時に、次期シード値が検索され、シードとして用いられ、また、要求される乱数ランの長さがパラメータ「長さ」の値を得るために値１２８に加算される。プロセスはこういう風に連続する。もし、キー生成アルゴリズムが図７の方法を用いてＲＳＡキーを生成するならば、図７でステップ１６１，１６４，１７０に入る時には、ＫＧＡ１５２は動的にシードされる擬似乱数発生器２００にコールする必要がある。必要となる乱数ＲＮ１，ＲＮ２等の長さはモジュラスの望みの長さにより、またＫＧＡおよび暗号システム自体の特定の実行によって変る。

【００５３】本発明はかかる環境のすべてにおいて、またＲＳＡアルゴリズム、ＲＳＡキー生成アルゴリズム、ＲＳＡ暗号システムの実行において実践できることは当業者は認めるであろう。さらに、これら他のアルゴリズムによるキー生成が、キー生成に含まれるステップがプロセス中のある時点、時期に、動的にシードされる擬似乱数発生器２００により生成しうる乱数または無作為値を要求しているという点で、ＲＳＡアルゴリズムのキー生成と類似であることを、公用キーアルゴリズムに詳しい人は認めるであろう。このように、本発明はＲＳＡキーの作成のみに限定されず、一般的にパスフレーズから公用キーおよび私用キーを生成する方法が、他の公用キーアルゴリズムに同様に拡張することを当業者は認めるであろう。ＫＧＡ１５２がキー生成プロセスを完了後、すなわちＰＵ、ＰＲが生成された後、ＰＵとＰＲはＧＰＵＰＲ命令５２に５４でリターンされる。応答して、ＧＰＵＰＲ命令５２はＰＵ、ＰＲおよび５０で入力として供給されたモードおよび制御ベクトルを用いてＰＵキートークンおよびＰＲキートークンを構成する。次に既に述べたように、ＧＰＵＰＲ命令５２は５０で入力として供給されたモードおよび制御ベクトルに一貫性チェックを実行し、キータイプおよび使用法がキー生成法に一致しているかどうか（すなわちパスフレーズに基づいているか、パスフレーズに基づいていないか）を判定する。一貫性チェックにパスすれば、ＰＵキートークンとＰＲキートークンは５１でＣＦＡＰ（キー生成機能）にリターンされる。一方も、一貫性チェックにパスしないと、ＧＰＵＰＲ命令５２は停止し、ＰＵキートークンとＰＲキートークンは５１でＣＦＡＰにリターンされない。

【００５４】パスフレーズ選択プロセス：ユーザにより入力として供給される機密のパスフレーズから、公用キーおよび私用キーペア（ＰＵ、ＰＲ）を生成するための、本発明の方法を述べてきた。この結果の私用キーＰＲは入力したパスフレーズの値に完全に依存しており、またキー生成アルゴリズムは公用の知識であると仮定しているので、私用キーＰＲの機密保護は完全にパスフレーズそのものの機密保護に依存するものと推測される。敵が誰かのパスフレーズの入手または推測することが可能だとしたら、その敵は既知のキー生成アルゴリズムとパスフレーズを用いて私用キーＰＲを決定できるであろう。ユーザのパスフレーズの機密を保護するのに用いなければならない方策に２つの基本分類がある。即ち：

・選択したパスフレーズを無許可のパーティに開示することを防止する方策と、

・無許可のパーティが選択したパスフレーズを単純推定することを防止する方策である。

【００５５】第１分類の方策は一般にはユーザに原則や指針のセットを提供することにより実行される。例えば、パスフレーズは記憶すべきでメモすべきでない。もしパスフレーズをメモするなら、不慮の開示を避けるため管理された環境の下で行わなければならない。さらにメモしたコピーは不使用時は確実に保管しなければならない。これら規則の大部分は常識そのものであり、システムパスワード、錠の組合せ、私用電話番号の取扱いのような毎日ユーザが扱っている多くの「秘密」に適用されるものである。

【００５６】第２分類の方策は常識の原則から明示するのはより困難なことが多い。この方策はユーザがパスフレーズ自体を選択するのに用いる方法に焦点をおく。パスフレーズは他より推定が容易なことは明白である。従って、「良い」パスフレーズ（すなわち容易に推定できないもの）を選択し、「悪い」パスフレーズ（すなわち、容易に推定できるもの）を回避する体系的方法が提供さるべきである。

【００５７】図１７にパスフレーズ選択プロセスを示す。第１ステップ３００は、パスフレーズ選択の原則と指針のセットを準備し発行することである。パスフレーズ選択指針はユーザが「良い」パスフレーズを選択するのを助けるために、ユーザに提供される。これら原則には後章で述べるようにパスフレーズ「フィルタ」を満足するような基準のセットが書面で分り易い様式で含まれている。

【００５８】パスフレーズ選択指針の見本：本章では適切なパスフレーズ作成をユーザに指導するため「べし」と「べかず」のリストを提供する。良い選択と悪い選択とを説明する特定の実施例が与えられる。敵がこの文書を見ていることもあり得るので、実際にはいずれの見本も使用すべきではない。

【００５９】基本的にパスフレーズは「構成」しなければならない：敵が推定する恐れのあるレパートリーのフレーズから選択してはならない。さらに、パスワードの構成に当っては語の「数」および語の使用「頻度」は、実用上、敵が大規模、指向性探索を用いてもパスワードを発見できないようなものにする。

【００６０】「悪い」パスワード（例えば、自分の名前とか電話番号）を使用すると、無作為に生成されているような見かけを有する暗号キーを作成し、この意味では偶然の侵入者に対してはある程度の保護を与える。しかし、こういったキーは真の暗号保護を与えない。

【００６１】避けるべき習慣（過去にこれらを使用して実際に暗号文が解読されたことがある）は次の通りである。

【００６２】１．　パスフレーズを自分自身で構成する代りに、パスフレーズリスト（例：a book）からパスフレーズを選択しないこと。

【００６３】２．　フレーズの中の数語が残りの手がかりを与えるような推測のできるフレーズを用いないこと。例えば

・　よく知られている詩や子守歌からの１行

・　よく知られている人、場所、事柄の名前

・　国家、文化、民族、宗教的ヘレディティからのフレーズを使用しないこと。

【００６４】３．　以前のパスフレーズと同じ概念のフレーズを使用しないこと。例えば、もし前回、祖父に関することを用いたとしたら、今回は祖母に関することを用いないこと。

【００６５】４．　パスフレーズとして１語だけというのは使用しないこと。平均的辞書には約１０，０００語含まれている。この多様性は２の１４乗以下であり、荒予的速度では直ぐに究明できる。

【００６６】５．　最も普通の英語の単語「のみ」を使用しないこと。（すなわち、アングロサクソン起源の基本語）。こうすると敵の辞書のサイズは１０，０００語以上から、約２，０００語またはそれ以下に減らすことができよう。

【００６７】６．　小学校の教科書にある文を使用しないこと。効力のある習慣は次の通りである。

【００６８】１．　パスフレーズは新規に創造すること（すなわち、オリジナルであるべきである）

２．　パスフレーズの長さはアルファベット文字（Ａ～Ｚ）で空白を除き少くとも４０～５０文字のこと。これで約１０語になり、徹底的なコンピュータ解析を妨げるのに充分である。

【００６９】３．　次の１個あるいはそれ以上を行うことにより、敵が必要とするアルファベットまたは辞書を増加させることを考えること。

【００７０】・　特殊記号を含めること（例えば、自分のキーボードにもよるが、‖＠＃＄％「＆＊（）＿＋－＝！¢：；，．？″′＼｜｛｝＜＞）

・　文章に数字を導入すること。

【００７１】・　故意に単語をミススペルすること。
（例：happen 3 stance ）

・　外国語を使用すること。入力記号のセット
を増し、またパスフレーズの各記号は、２６可能性の文字の代りに、ずっと多くの可能性の文字数字記号を有することになる。もちろんパスフレーズが記憶困難になるという事実によりこの実施の阻害されることがある。

【００７２】４．　パスフレーズに固有名前を含んでいても支障ない。

【００７３】５．　パスフレーズを記憶し易くするよう努め、書き留める必要がないようにすること。逆にフレーズは他の誰かが推定することができなくすべきで、自分だけが知っている内輪の情報を含めることを考えること。

【００７４】パスフレーズの例：
悪いパスフレーズの例：

・「Antidisestablismentarianism」－単一の辞書語
・「Dick and Jane see Spot run. Jump Spot jump.」－小学１年の教科書
・「A bee bit me.」－短かすぎる
・「George Washington Carrer」－有名人
・「Mary had a little l amb, ifs fleece was white as snow.」－有名な諺
・「Thon shalt have no other gods before Me.」－宗教的ヘリテージ
・「Four score and sever years ago…」－国家的伝統

良いパスフレーズの例：

・「I have never lived in Chicago at 278 Lake Shore.」
・「Why do you believe that fishies dan't float in the sky?」
・「Did George Washington read Pascal or talk to an ambassdor?」
・「My favorite color is green or am I lieing &; it's Moorish Mist.」
・「Counting"won, too, tree" is childish (but so what)!」
・「Cannot I dance on my head? I dunno, perhaps I shall.」

パスフレーズフィルタ：再び図１７を参照し、ユーザがステップ３０１でパスフレーズを一旦選択すると、その選択の良否を判断するために発行されている選択指針に対しユーザ選択を評価することは有益である。この評価プロセスには指針と原則３００で発行されているもの以上の追加基準をお勧めすることがある。追加基準を原則の形で述べるのは困難かも知れないが、それにも拘らず選択したパスフレーズの質を判定するには重要である。総合評価基準として、試用パスフレーズを入力し３０１、試用パスフレーズをテストし３０２、テスト３０２の結果を基にして試用パスフレーズを受託または拒否する３０３、といった具合に自動化することもできる。３０３で受託されると、順に次のキー生成プロセスの使用可能をトリガする。拒否されるとエラーメッセージをトリガし、ユーザに別のフレーズを選択するよう促す。パスフレーズテスト３０２はパスフレーズフィルタの形で実行することがある。

【００７５】パスフレーズフィルタは「悪い」ユーザ構成のパスフレーズすなわち敵が徹底した指向探索により発見できる可能性のあるパスフレーズを拒否するためのルーチンである。可能性のあるパスフレーズが生成されると、パスフレーズフィルタが呼び出され、パラメータ入力としてパスフレーズが提供される。最も頻繁に使用される１０，０００語を含む標準英語の辞書を用いて、パスフレーズフィルタは敵のコンピュータプログラムがユーザのパスフレーズを再生成するまでに通常列挙しなければならないパスフレーズ数の下限を計算する。この情報は呼び出し者に報告され、パスフレーズの放棄、修正、受託を呼出し者が選ぶことができる。

【００７６】パスフレーズフィルタはそのパスフレーズが「良い」ことを自動的に保証するものではないが、大抵の「悪い」パスフレーズを消去することができる。この意味でパスフレーズ構成用に提供された原則と共にパスフレーズフィルタを用いると、「悪い」パスフレーズが不注意に用いられる機会を最小化し、従って全体の機密保護が向上する。

【００７７】パスフレーズフィルタは概念的にはパスワードフィルタと類似しており、「悪い」ユーザ設定のパスフレーズまたは徹底した指向探索により敵が発見できる可能性のあるパスフレーズを拒否するルーチンである。

【００７８】パスフレーズを含む例がこのチェック手順の重要性を説明している。ユーザ選定のパスフレーズのような、ユーザ選定のパスワードはよりユーザに親しみ易いアクセス制御とのインタフェースを与える。しかし人間は「容易な道を選ぶ」傾向があることはよく知られている。１０００人が選んだ６桁のパスワードを調べてみると、その分布が一様ではないことは確実である。６個の繰返し数字（０００００、１１１１１等）、順番の数字（１２３４５６、２３４５６７等）または明白なパターンの数字からなるパスワードが不釣合に多いことに気付くであろう。これを知っていると、敵は最もありそうな候補を最初に探索するように徹底した指向探索を組織化できる。多くの場合には、パスワードを見付けるにほんの僅かの試行しか必要としない。対策として、パスワード選択に含まれる潜在的リスクについてユーザに伝えておかなければならないし、またコンピュータシステムの導入においてはパスワード選択において守るべき簡単な原則をセットでユーザに提供しなければならない。弱いパスワードをテストし拒否するために多くのコンピュータシステムではパスワードチェックアルゴリズムを提供することも可能である。

【００７９】パスフレーズ構成においては、煩似しているが、より複雑な原則のセットを守らなければならない。多くの場合、原則は直観的ではなく、従って、システムに実行されるパスフレーズフィルタは尚更重要である。パスフレーズフィルタは試用パスフレーズに適用される簡単な高速テストのセットからなる。各テストはパスフレーズの変異性を評価する。すべてのテストを実行後、最小値をユーザに報告する。

【００８０】図１８には、暗号命令セット２を実行可能な暗号化機構し、キー記憶装置３、暗号化機構アクセスプログラム４、ユーザアプリケーションプログラム５よりなる暗号システムを示す。暗号化機構アクセスプログラム４はパスフレーズフィルタユーティリティプログラム６を含み、チェックパスフレーズ７と呼ばれるＣＦＡ

Ｐサービスを通してアクセスされる。試用パスフレーズをチェックするのに次のステップが含まれる。アプリケーション５がチェックパスフレーズサービス７を呼び出す。試用パスフレーズをチェックし、パスフレーズの変異性推定を呼出し者にリターンする。呼出し者は受託のための最小変異性を設定しなければならない。例えばＤＥＡキー生成に対しては、変異性は最小２の５６乗であるべきである。

【００８１】図１９はパスフレーズフィルタルーチンの処理ステップの流れ図である。パスフレーズフィルタは次のチェックを行う。

【００８２】１．　パターン分析－記号または記号列が繰返されているか？

２．　文字頻度分析－個々の文字、２重字、３重字等が如何なる頻度で典型的な言語では表われ、また提案のパスフレーズに限定するとどうか？

３．　ワード頻度分析－特定のワードが如何なる頻度で表われるか？

パスフレーズフィルタによりユーザに報告されるパスフレーズの推定変異性は上記分析のそれぞれから得られる変異性の最小値である。これら分析の実行方法を以下に述べる。

【００８３】パターン分析：試用パスフレーズの標準統計分析で次のことが分る。

【００８４】１．　パスフレーズに用いられた全アルファベット

２．　文字または文字グループの繰返し

このデータから、統計的変異性の計算が容易にできる。例えば、「有効アルファベット」がパスフレーズ中に表わる記号のみで構成されると仮定し、またパスフレーズの「有効長さ」をすべての繰返しを除いたパスフレーズの長さと定義せよ。そうすると「ＩＩＩＩＩＩ」のようなパスフレーズは「悪い」と分類するであろう。

【００８５】数字や文字の自然の順番もある。この自然の順番を用いると、パスフレーズは敵に推測されうるかも知れない。数字やアルファベット順を検知する一方法は各数字および文字にランク番号を割り当て、有限差分計算法を用いることである。この方法は有限個数の指定点を通る多項式の次数を計算するのに使われる方法である。この方法を以下に示す。

【００８６】１．　数字０～９にランク番号１～１０を割り当て、文字「Ａ」～「Ｚ」にランク番号１１～３６を割り当てる。

【００８７】２．　パスフレーズに対するランク番号のリストを生成する。

【００８８】３．　左端から始めて、各要素から直ぐ右側の要素を減算し、一次差分を計算する。リストの最後の数字はそれに対し計算すべき差分を有しない。

【００８９】４．　一次差分の数に同じ操作を行って二次差分を計算する。

【００９０】例えば、パスフレーズを次のように仮定し、

パスフレーズ：１　２　３　４　５

ランク番号：　０２　０３　０４　０５　０６

一次差分：　　０１　０１　０１　０１

二次差分：　　００　００　００

一次差分のリストにおいて入力がゼロの時は、隣接したランク番号が同一であることを意味する。二次差分のリストにおいて入力がゼロの時は一次差分が同一すなわちランク番号が定数だけ変化していることを意味し、パスフレーズの１片が「２４６」とか「ＡＢＣ」のような順序になっていることを意味する。可変性計算では、パスフレーズの有効長さは一次および二次差分リストにあるゼロの数だけ減算される。（このようなゼロは繰返しまたは単純パターンを示すので）。

【００９１】このランク番号分析は「qwerty」（または他の）キーボードの数字と文字の順番でもって行うことも可能である。

【００９２】文字頻度分析：次の文字リストはGaimes（参考文献２）からとったものである。

【００９３】英文での文字の頻度順リストは、

ＥＴＡＯＮＩＳＲＨＬＤＣＵＰＦＭＷＹＢＧＶＫＱＸＪＺ。

【００９４】もし特殊記号が含まれるとすれば、その時は最も普通の記号（「Ｅ」よりもさらに）はブランクすなわちスペースである。英文での２重字の頻度順リストは

ＴＨ　ＨＥ　ＡＮ　ＩＮ　ＥＲ　ＲＥ　ＥＳ　ＯＮ　ＥＡ　ＴＩ　ＡＴ　ＳＴＥＮ　ＮＤ　ＯＲ　ＴＯ　ＮＴ　ＥＤ　ＩＳ　ＡＲ…

英文での３重字の頻度順リストは

ＴＨＥ　ＡＮＤ　ＴＨＡ　ＥＮＴ　ＩＯＮ　ＴＩＯ　ＦＯＲ　ＮＤＥ　ＨＡＳＮＣＥ　ＥＤＴ　ＴＩＳ　ＯＦＴ　ＳＴＨ　ＭＥＮ…

１．　各文字を頻度グループにグループ分けして、各グループに変異性の推定値を与える。簡単のため、グループの変異性は２の整数べきであるようにグループを定義する。

【００９５】ａ．　２の０乗　（２＊＊０）　Ｅ

ｂ．　２の１乗　（２＊＊１）　Ｔ

ｃ．　２の２乗　（２＊＊２）　ＡＯ

ｄ．　２の３乗　（２＊＊３）　ＮＩＳＲ

ｅ．　２の４乗　（２＊＊４）　ＨＬＤＣＵＰＥＭ

ｆ．　２の５乗　（２＊＊５）　ＷＹＢＧＶＫＱＸＪＺ

ｇ．　ブランク以外の特殊記号には２の５乗の値を付ける。

【００９６】２．　パスフレーズにおける文字の繰返しパターンをチェックし、分析しようとするパスフレーズから繰返しパターンを取り除く。

【００９７】３．　分析しようとするパスフレーズから

すべてのブランクを取り除く。

【００９８】４．　（パターンを取り去った後の）各文字に対応する２のべき指数を合計する。合計値がこのテストの変異性である。

【００９９】５．　２重字および３重字についても同じことを行う。

【０１００】ワード頻度分析：以下はJohn B. Carrollの「The American Heritage WordFrequency Book」（１９７１）からとったものである。最も普通の英語１００ワードの頻度順リストは以下の通りである。

【０１０１】THE OF AND A TO IN IS YOU THAT IT HE FOR WAS ON ARE AS WITH HIS THEYAT BE THIS FROM I HAVE OR BY ONE HAD NOT BUT WHAT ALL WERE WHEN WE THERECAN AN YOUR WHICH THEIR SAID IF DO WILL EACH ABOUT HOW UP OUT THEM EHENSHE MANY SOME SO THESE WOULD OTHER INFO HAS MORE HER TWO LIKE HIM SEETIME COULD NO MAKE THAN FIRST BEEN ITS WHO NOW PEOPLE MY MADE OVER DIDDOWN ONLY WAY FIND USE MAY WATER LONG LITTLE VERY AFTER WORDS CALLEDJUST WHERE MOST KNOW

最も頻繁に使われる１０，０００ワードを含む標準英語の語彙を用い、ユーザのパスフレーズを再生成するまでに敵のコンピュータプログラムが列挙しなければならないであろうパスフレーズ数の下限をユーティリティプログラムが計算する。

【０１０２】１．　次のようにワード頻度リストを構築する。

【０１０３】ａ．　２の０乗　（２**０）　THE

ｂ．　２の１乗　（２**１）　OF

ｃ．　２の２乗　（２**２）　AND　A

ｄ．　２の３乗　（２**３）　TO　IN　IS　YOU

ｅ．　２の４乗　（２**４）　THAT　IT　HE　FOR　WAS　ONARE　AS

ｆ．　等々

所望の長さにワード頻度リストに対するこのリストを構築する。あるワードがそのリストに現れなければ、そのリストの最少頻度ワードと同じ頻度を有するものと仮定する。

【０１０４】２．　繰返しワードをチェックし、分析しようとするパスフレーズから繰返しワードを取り除く。

【０１０５】３．　パスフレーズの各ワードに対応する２のべき指数を合計する。合計値がこのテストの変異性である。

【０１０６】本発明の特定の実施例を開示したが、本発明の精神および目的から逸脱することなく、特定の実施例に変更を行いうることは当業者には自明である。

【０１０７】本発明の公用キー暗号システムを管理する方法は、ユーザに知られている第１のシード値を用いて第１の公用キー、私用キーペアを生成し、また第１の公用キー、私用キーペアの第１の使用を定義する第１の制御ベクトルを生成するステップと、ユーザに知られている第２のシード値を用いて第２の公用キー、私用キーペアを生成し、また第２の公用キー、私用キーペアの第２の使用を定義する第２の制御ベクトルを生成するステップと、第１の制御ベクトルを用いて第１の公用キー、私用キーペアの使用を制御ベクトルするステップと、第２の制御ベクトルを用いて第２の公用キー、私用キーペアの使用を制御ベクトルするステップとを含んでいる。

【０１０８】ここで、第１のシード値がパスフレーズから生成されてもよく、第２のシード値が真の乱数であってもよい。また、第１のシード値を用いて第１の乱数を生成し、第１の生成ステップに第１の乱数を適用するステップを含んでもよい。さらに、擬似乱数発生器に前記第２のシード値を用いて第２の乱数を生成し、第２の生成ステップに第２の乱数を適用してもよい。

【０１０９】また、第１の制御ベクトルが２つの構成要素として、第１の公用キーの使用を制御するための第１の公用キー制御ベクトルおよび第１の私用キーの使用を制御するための第１の私用キー制御ベクトルを有してもよい。

【０１１０】あるいは、第２の制御ベクトルが２つの構成要素として、第２の公用キーの使用を制御するための第２の公用キー制御ベクトルおよび第２の私用キーの使用を制御するための第２の私用キー制御ベクトルを有してもよい。

【０１１１】第１の制御ベクトルが第１の私用キーを制御してその使用をディジタル署名の生成に制限しまた第２の制御ベクトルが第２の私用キーを制御して、その使用をディジタル署名の生成に制限し、かつキー分散プロトコルの一部として受信した暗号化されたキーを解読してもよい。

【０１１２】または、第１の制御ベクトルが第１の公用キーの使用をディジタルシグニチャの検証に制限し、また第２の制御ベクトルが第２の公用キーの使用をディジタルシグニチャの検証およびキー分散プロトコルにおけるキーの暗号化に制限してもよい。

【０１１３】あるいは、第１の制御ベクトルは第１の私用キーによりディジタルシグニチャの生成を制御し、また第２の制御ベクトルは第２の私用キーの使用をディジタルシグニチャの生成には禁止してもよい。

【０１１４】また本発明の公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法は、ユーザに知れている第１のシードを用いて第１の公用キー、私用キーペアを生成し、また第１の公用キー、私用キーペアの第１の使用を定義する第１の制御ベクトルを生成するステップと、ユーザに知れない第２のシード値を用いて第２の公用キー、私用キーペアを生成し、また第２の公用キー、私用キーペアの第２の私用キーペアを定義する第２の制御ベクトルを生成するステップと、第１の制御ベクトルを用いて第１の公用キー、私用

キーペアの使用を制御するステップと、第２の制御ベクトルにより第２の公用キー、私用キーペアの使用を制御するステップとを含んでいる。

【０１１５】ここで、第１のシード値がパスフレーズから生成されてもよく、また第２のシード値が真の乱数であってもよい。

【０１１６】また、第１のシード値を用いて第１の乱数を生成し、また第１の生成ステップに第１の乱数を適用するステップの遂行を含んでもよい。

【０１１７】あるいは、擬似乱数発生器における第２のシード値を用いて第２の乱数を生成し、また第２の生成ステップに第２の乱数を適用するステップの遂行を含んでもよい。

【０１１８】第１の制御ベクトルが２つの構成要素として、第１の公用キーの使用を制御するための第１の公用キー制御ベクトルおよび第１の私用キーの使用を制御するための第１の私用キー制御ベクトルを有してもよい。

【０１１９】第２の制御ベクトルが２つの構成要素として、第２の公用キーを制御するための第２の公用キー制御ベクトルおよび第２の私用キーを制御するための第２の私用キー制御ベクトルを有してもよい。

【０１２０】第１の制御ベクトルが、第１の私用キーを制御して、その使用をディジタル署名の生成に制限し、また第２の制御が第２の私用キーを制御して、その使用をディジタル署名の生成およびキー分散プロトコルの一部として受信した暗号化されたキーの解読を制限してもよい。

【０１２１】第１の制御ベクトルが、第１の公用キーの使用をディジタル署名の検証に制限し、また第２制御ベクトルが第２公用キーの使用をディジタル署名の生成およびキー分散プロトコルにおけるキーの暗号化を制限してもよい。

【０１２２】第１制御ベクトルが第１私用キーでもってディジタル署名の生成を制御ベクトルし、また第２制御ベクトルが第２私用キーの使用がディジタル署名の生成を行うことを禁止してもよい。

【０１２３】本発明の公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置は、ユーザに知られる第１シード値を用いて第１公用キー、私用キーペアを生成し、また第１公用キー、私用キーペアの第１使用を定義する第１制御ベクトルを生成する第１生成手段と、ユーザに知られない第２シード値を用いて第２公用キー、私用キーペアを生成し、また第２公用キー、私用キーペアの第２使用を定義する第２制御ベクトルを生成する第２生成手段と、第１制御ベクトルを用いて第１公用キー、私用キーペアの使用を制御するための、第１生成手段に連結される制御手段と、第２制御ベクトルにより第２公用キー、私用キーペアの使用を制御するための、第２生成手段に連結される制御手段とを含んでいる。

【０１２４】ここで、第１シード値がパスフレーズから生成されてもよく、第２シード値が真の乱数であってもよい。

【０１２５】第１生成手段が、第１シード値を用いて第１乱数を生成し、また第１公用キー、私用キーペアの生成に第１乱数を適用してもよい。

【０１２６】第２生成手段が、擬似乱数発生器において第２シード値を用いて第２乱数を生成し、また第２公用キー、私用キーペアの生成に第２乱数を適用してもよい。

【０１２７】第１制御ベクトルが２構成要素として、第１公用キーの使用を制御するための第１公用キー制御ベクトルおよび第１私用キーの使用を制御するための第１私用キー制御ベクトルを有してもよい。

【０１２８】第２制御ベクトルが２構成要素として、第２公用キーの使用を制御するための第２公用キー制御ベクトルおよび第２私用キーを制御ベクトルするための第２私用キー制御ベクトルを有してもよい。

【０１２９】第１制御ベクトルが第１私用キーの使用をディジタル署名の生成に制限するよう第１私用キーを制御し、また第２制御ベクトルが第２私用キーの使用をディジタル署名の生成およびキー分散プロトコルの一部として受信される暗号化されたキーの解読に制限するよう第２私用キーを制御してもよい。

【０１３０】第１制御ベクトルが第１公用キーの使用をディジタル署名の検証に制限し、また第２制御ベクトルが第２公用キーの使用をディジタル署名の検証およびキー分散プロトコルにおけるキーの暗号化を制限してもよい。

【０１３１】第１制御ベクトルは第１私用キーでもってディジタル署名の生成を制御し、第２制御ベクトルは第２私用キーの使用がディジタル署名の生成を禁止してもよい。

【図面の簡単な説明】

【図１】ユーザｉ，ｊが共用する暗号システムＡにおいてパスフレーズから公用キーおよび私用キーペア生成を説明するブロック図。

【図２】ユーザｉによる暗号システムＡおよびＢにおいてパスフレーズから公用キーおよび私用キーペア生成を説明するブロック図。

【図３】各々が暗号システムを含む多数のデータ処理装置を含む通信ネットワーク１０の説明図。

【図４】暗号システム２２の構成を示すブロック図。

【図５】暗号化機構３０の構成を示すブロック図。

【図６】暗号化機構３０の暗号アルゴリズム１４４の構成要素のブロック図。

【図７】ＲＳＡキー生成に含まれるステップを説明する暗号化機構３０のキー生成アルゴリズム１５１の構成要素のブロック図。

【図８】「真の」乱数発生器１８０を説明するブロック

図。

【図９】初期にシードされる擬似乱数発生器１９０を説明するブロック図。

【図１０】動的にシードされる擬似乱数発生器２００を説明するブロック図。

【図１１】本発明により動的にシードされる擬似乱数発生器２００を含むように修正された、暗号化機構３０の暗号アルゴリズム１４４構成要素のブロック図。

【図１２】動的にシードされる擬似乱数発生器の特定例を説明するブロック図。

【図１３】本発明に従って入力パスフレーズから公用キーおよび私用キーペアの生成に含まれるステップを示すブロック図。

【図１４】本発明に従って公用キーおよび私用キーペア生成（ＧＰＵＰＲ）命令を説明するブロック図。

【図１５】ＰＵキーおよびＰＲキートークンを説明するブロック図。

【図１６】ＰＵ、ＰＲキートークンの制御ベクトル部分を説明するブロック図。

【図１７】パスフレーズ選択プロセスを説明するブロック図。

【図１８】ユーザアプリケーションが提供する試用パスフレーズテストのためのパスフレーズフィルタを用いる暗号システムを説明するブロック図。

【図１９】パスフレーズフィルタの機能要素を説明するブロック図。

【符号の説明】

１，３０　暗号化機構（ＣＦ）

２　暗号命令セット

３　キー記憶装置

４　暗号化機構アクセスプログラム

５　ユーザアプリケーションプログラム

６　パスフレーズフィルタユーティリティプログラム

７　チェックパスフレーズサービス

１０　通信ネットワーク

２０　データ処理装置

２２　暗号システム

３２　暗号キーデータセット（ＣＫＤＳ）

３４　暗号化機構アクセスプログラム（ＣＦＡＰ）

３６　アプリケーションプログラム（ＡＰＰＬ）

４２　アプリケーションプログラムＡ（ＡＰＰＬ　Ａ）

４３，４４，４５

４６　キー記憶装置マネージャ

４７　キー生成機能

４８　キーパージ機能

５２　ＧＰＵＰＲ命令

１４０　機密保護範囲

１４２　命令処理装置

１４４，１５０　暗号アルゴリズム

１４６　暗号化機構環境記憶装置

１５１　キー生成アルゴリズム（ＫＧＡ）

１５２　乱数生成アルゴリズム

１８０　「真」乱数発生器

１８１　ハードウエア回路

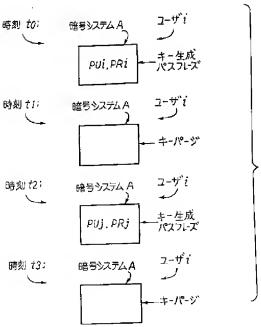
１９０　初期にシードされる擬似乱数発生器

１９１，２０１　アルゴリズム

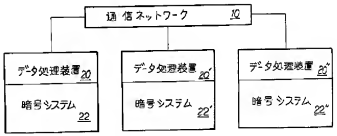
１９４　シード記憶装置

２００　動的にシードされる擬似乱数発生器

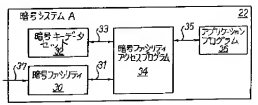
【図１】



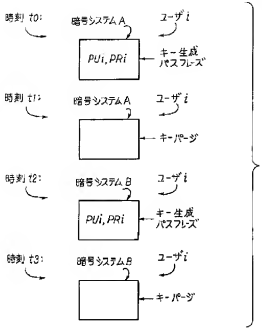
【図３】



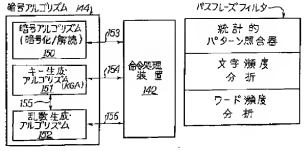
【図４】



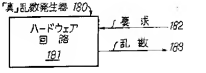
【図２】



【図６】

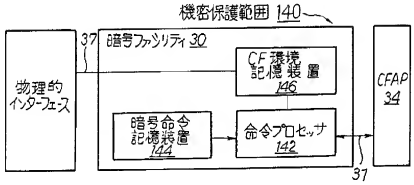


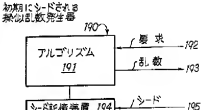
【図８】



【図９】

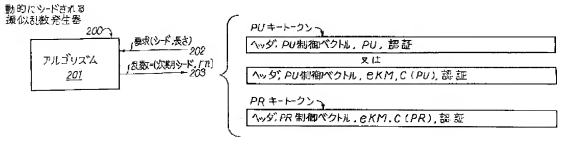
【図５】



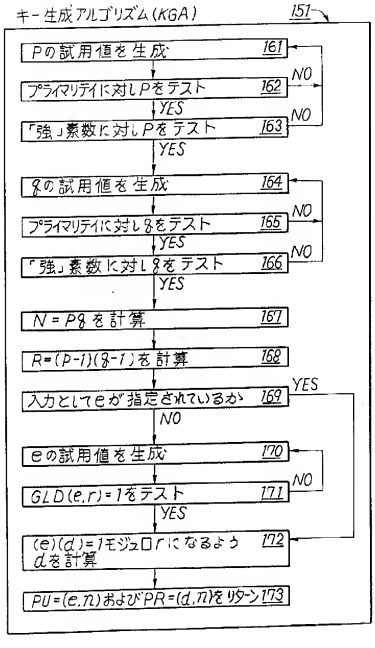


【図１０】

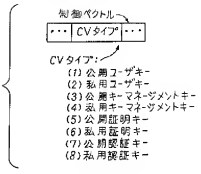
【図１５】



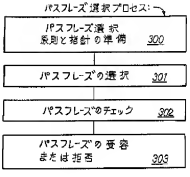
【図７】



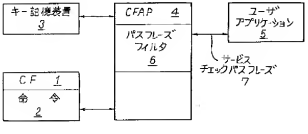
【図１６】



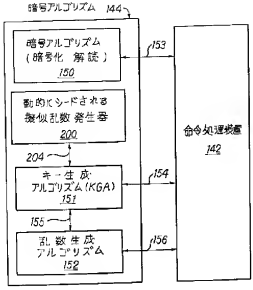
【図１７】



【図１８】



【図１１】



【図１２】

動的にシードされる擬似乱数発生器

入力

m　：生成されるべき乱数の長さをビットで表わす正の整数

シード　：124ビット値

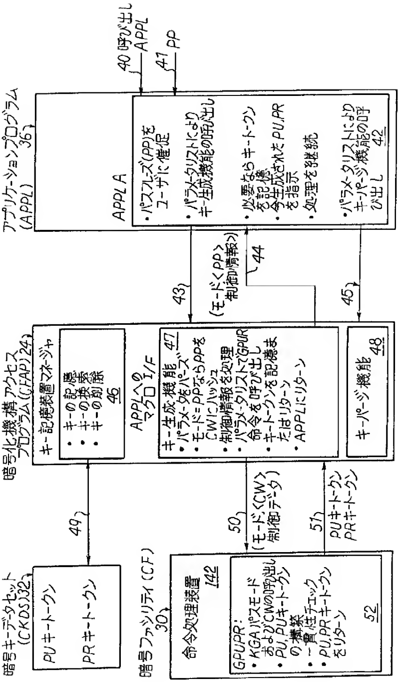
出力

RN　：生成された長さMビットの乱数

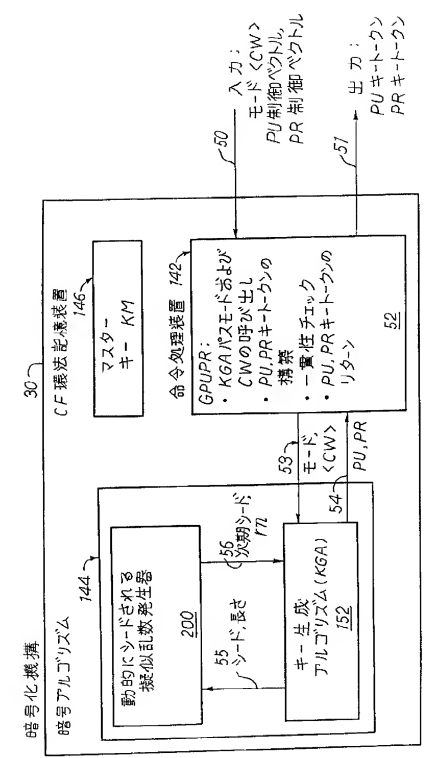
アルゴリズムの仕様

1. nをセット；$n=m\div 64$
2. nを次の最大正の整数に丸める
3. Kをセット：Kはシードの最も重要な(最左端の)64ビット
4. ICVをセット：ICVはシードの最も重要でない(最右端の)64ビット
5. Aをセット：AはゼロビットのNブロック
6. Yをセット：YはキーK，初期の連鎖値がICV
   において，暗号化の暗号ブロック連鎖モードを用い，
   データ暗号化アルゴリズムによりAを暗号化する
   時に作成される暗号文
7. RNをセット；RNはYの最も重要な(最左端)のmビット

【図１３】


アプリケーションプログラム(APPL) 36
APPL A
・パスフレーズ(PP)をユーザに催促
・パラメータリストによりキー生成機能の呼び出し
・必要ならキートークンを記憶
・今生成されたPU,PRを指示
・処理を継続
・パラメータリストによりキーパージ機能の呼び出し
42
40 呼び出しAPPL
41 PP
43
(モード<PP> 制御情報)
44
45
暗号化機構アクセスプログラム(CFAP) 24
キー記憶装置マネージャ
・キーの記憶
・キーの検索
・キーの削除
46
APPLへのマクロI/F
キー生成機能 47
・パラメータをパーズ
・モード=PPならPPをCWにハッシュ
・制御情報を処理
・パラメータリストでGPUR命令を呼び出し
・キートークンを記憶またはリターン
・APPLにリターン
キーパージ機能
48
49
50 (モード,<CW> 制御データ)
51 PUキートークン PRキートークン
暗号キーデータセット(CKDS) 32
PUキートークン
PRキートークン
暗号ファシリティ(CF) 30
命令処理装置 142
GPUPR:
・KGAパスモードおよびCWの呼出し
・PU,PUキートークンの構築
・一貫性チェック
・PU,PRキートークンをリターン
52

【図１４】


暗号化機構
30
CF擬似乱数発生器
146
暗号アルゴリズム
144
マスター
キー KM
動的にシードされる
擬似乱数発生器
200
55
シード, 長さ
55
次期シード
IV
キー生成
アルゴリズム(KGA)
152
命令処理装置 142
GPUPR:
・KGAパスモードおよび
CWの呼び出し
・PU,PRキートークンの
操作
・一貫性チェック
・PU,PRキートークンの
リターン
52
53
モード,
<CW>
54
PU,PR
50
入力:
モード<CW>
PU制御ベクトル,
PR制御ベクトル
51
出力:
PUキートークン
PRキートークン

【手続補正書】
【提出日】平成４年１１月１６日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、
ユーザに知られている第１のシード値を用いて第１の公用キー、私用キーペアを生成し、また前記第１の公用キー、私用キーペアの第１の使用を定義する第１の制御ベクトルを生成するステップと、
ユーザに知られている第２のシード値を用いて第２の公用キー、私用キーペアを生成し、また前記第２の公用キー、私用キーペアの第２の使用を定義する第２の制御ベクトルを生成するステップと、
前記第１の制御ベクトルを用いて前記第１の公用キー、私用キーペアの使用を制御するステップと、
前記第２の制御ベクトルを用いて前記第２の公用キー、私用キーペアの使用を制御するステップとを含むことを特徴とする方法。
【請求項２】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理する方法であって、
パスフレーズから導出される第１のシード値を用いて第１の乱数を生成するステップと、
ユーザには知られない第２のシード値を用いて第２の乱数を生成するステップと、
前記第１の乱数を用いて第１の公用キー、私用キーペアを生成し、また前記第１の公用キーおよび前記第１の私用キーの第１の使用を定義するために、それぞれ第１の公用キー制御ベクトルおよび第１の私用キー制御ベクトルを生成するステップと、
前記第２の乱数を用いて第２の公用キー、私用キーペアを生成し、また前記第２の公用キーおよび前記第２の私用キーの第２の使用を定義するために、それぞれ第２の公用キー制御ベクトルおよび第２の私用キー制御ベクトルを生成するステップと、
前記第１の公用キー制御ベクトルおよび前記第１の私用キー制御ベクトルを用いて、それぞれ前記第１の公用キーおよび前記第１の私用キーの使用を制御するステップと、
前記第２の公用キー制御ベクトルおよび前記第２の私用キー制御ベクトルを用いて、それぞれ前記第２の公用キーおよび前記第２の私用キーの使用を制御するステップとを含むことを特徴とする方法。
【請求項３】データ処理システムにおいて、キー発生器を有する暗号システムを管理する方法であって、
パスフレーズから導出される第１のシード値を用いて第１の乱数を生成するステップと、
ユーザに知られない第２のシード値を用いて第２の乱数を生成するステップと、
前記第１の乱数を用いて第１キーを生成し、また前記第１のキーの使用を制御するための第１の制御ベクトルを生成するステップと、
前記第２の乱数を用いて第２のキーを生成し、また前記第２のキーの第２の使用を制御するための第２の制御ベクトルを生成するステップと、
前記第１の制御ベクトルにより前記第１のキーの使用を制御するステップと、
前記第２の制御ベクトルにより前記第２のキーの使用を制御するステップと、
前記第１のキーの前記第１の使用が、前記第２のキーの前記第２の使用と異なるステップとを含むことを特徴とする方法。
【請求項４】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出される第１のシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成し、前記第１の制御ベクトルは前記公用キーの使用を制御するもので、前記第２の制御ベクトルは前記私用キーの使用を制御するものであり、前記公用キーに対して前記第１の制御ベクトルを生成し、また前記私用キーに対して前記第２の制御ベクトルを生成するためのステップを含むことを特徴とする方法。
【請求項５】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出されるシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成するステップとを含むことを特徴とする方法。
【請求項６】データ処理システムにおいて、公用キー、私用キーペアを含む公用キー暗号システムを管理するための方法であって、
パスフレーズから導出される第１のシード値を用いて乱数を生成するステップと、
前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第１の制御ベクトルおよび前記私用キーに対する第２の制御ベクトルを生成し、前記第１の制御ベクトルが前記公用キーの使用を制御し、前記第２の制御ベクトルが前記私用キーの使用を制御するステップとを含むことを特徴とする方法。
【請求項７】データ処理システムにおいて、公用キー、

私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
ユーザに知られる第１シード値を用いて第１公用キー、私用キーペアを生成し、また前記第１公用キー、私用キーペアの第１使用を定義する第１制御ベクトルを生成する第１生成手段と、
ユーザに知られない第２シード値を用いて第２公用キー、私用キーペアを生成し、また前記第２公用キー、私用キーペアの第２使用を定義する第２制御ベクトルを生成する第２生成手段と、
前記第１制御ベクトルを用いて前記第１公用キー、私用キーペアの使用を制御するための、前記第１生成手段に連結される制御手段と、
前記第２制御ベクトルにより前記第２公用キー、私用キーペアの使用を制御するための、前記第２生成手段に連結される前記制御手段とを含むことを特徴とする装置。
【請求項８】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
パスフレーズから導出される第１シード値を用いて第１乱数を生成するための第１生成手段と、
ユーザに知られない第２シード値を用いて第２乱数を生成するための第２生成手段と、
前記第１乱数を用いて第１公用キー、私用キーペアを生成し、また前記第１公用キーおよび前記第１私用キーの第１使用をそれぞれ定義するための第１公用キー制御ベクトルおよび第１私用キー制御ベクトルを生成する前記第１生成手段と、
前記第２乱数を用いて第２公用キー、私用キーペアを生成し、また前記第２公用キーおよび前記第２私用キーの第２使用をそれぞれ定義するための第２公用キー制御ベクトルおよび第２私用キー制御ベクトルを生成する前記第２生成手段と、
前記第１公用キー制御ベクトルおよび前記第１私用キー制御ベクトルをそれぞれ用いて、前記第１公用キーおよび前記第１私用キーの使用を制御するための、前記第１生成手段に連結される制御手段と、
前記第２公用キー制御ベクトルおよび前記第２私用キー制御ベクトルをそれぞれ用いて、前記第２公用キーおよび前記第２私用キーの使用を制御するための、前記第２生成手段に連結される制御手段とを含むことを特徴とする装置。
【請求項９】データ処理システムにおいて、キー発生器を有する暗号システムを管理するための装置であって、
パスフレーズから導出される第１シード値を用いて第１乱数を生成するための第１生成手段と、
ユーザに知られない第２シード値を用いて第２乱数を生成するための第２生成手段と、
前記第１乱数を用いて第１キーを生成し、また前記第１キーの使用を制御するための第１制御ベクトルを生成する前記第１生成手段と、
前記第２乱数を用いて第２キーを生成し、また前記第２キーの第２使用を制御するための第２制御ベクトルを生成する前記第２生成手段と、
前記第１制御ベクトルでもって前記第１キーの使用を制御するための前記第１生成手段に連結される制御手段と、
前記第２制御ベクトルでもって前記第２キーの使用を制御するための前記第２生成手段に連結される前記制御手段と、
前記第１キーの前記第１使用が前記第２キーの前記第２使用と異なることを含むことを特徴とする装置。
【請求項１０】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
パスフレーズから導出される第１シード値を用いて乱数を生成する生成手段と、
前記乱数を用いて公用キー、私用キーペアを生成し、また前記公用キーに対する第１制御ベクトルおよび前記私用キーに対する第２制御ベクトルを生成し、前記第１制御ベクトルが前記公用キーの使用を制御し、前記第２制御ベクトルが前記私用キーの使用を制御する前記生成手段とを含むことを特徴とする装置。
【請求項１１】データ処理システムにおいて、公用キー、私用キーペア発生器を含む公用キー暗号システムを管理するための装置であって、
パスフレーズから導出されるシード値を用いて乱数を生成する生成手段と、
前記乱数を用いて公用キー、私用キーペアを生成する前記生成手段とを含むことを特徴とする装置。

フロントページの続き

(72)発明者　ドナルド、ビー、ジョンソン
アメリカ合衆国バージニア州、マナサス、クリスタル、クリーク、レーン、11635
(72)発明者　アン、ブイ、リ
アメリカ合衆国バージニア州、マナサス、バトルフィールド、ドライブ、10227
(72)発明者　ウィリアム、シー、マーティン
アメリカ合衆国ノースカロライナ州、コンコード、ヒリアード、レーン、1835
(72)発明者　ロスティスロー、プリマク
アメリカ合衆国バージニア州、ダンフリーズ、フェアウェイ、ドライブ、15900

(72)発明者　ジョン、ディー、ウィルキンズ
アメリカ合衆国バージニア州、サマービル、ピー、オー、ボックス、８